THE DISTRIBUTION OF THE FIRST ELEMENTARY DIVISOR OF THE REDUCTIONS OF A GENERIC DRINFELD MODULE OF ARBITRARY RANK

ALINA CARMEN COJOCARU AND ANDREW MICHAEL SHULMAN

Abstract. Let ψ be a generic Drinfeld module of rank $r \geq 2$. We study the first elementary divisor $d_{1,\wp}(\psi)$ of the reduction of ψ modulo a prime $\wp$, as $\wp$ varies. In particular, we prove the existence of the density of the primes $\wp$ for which $d_{1,\wp}(\psi)$ is fixed. For $r = 2$, we also study the second elementary divisor (the exponent) of the reduction of ψ modulo $\wp$ and prove that, on average, it has a large norm. Our work is motivated by the study of J.-P. Serre of an elliptic curve analogue of Artin's Primitive Root Conjecture, and, moreover, by refinements to Serre's study developed by the first author and M. R. Murty.

Contents

A.C. Cojocaru's work on this material was partially supported by the National Science Foundation under agreements No. DMS-0747724 and No. DMS-0635607, and by the European Research Council under Starting Grant 258713.

1. Introduction and statement of results

A beautiful and fruitful theme in number theory is that of exploring versions of one given problem in both the number field and function field settings. In many instances, such explorations unravel striking analogies, shedding light to deep basic principles underlying the problem. In other instances, the number field and function field versions of the same problem turn out to be surprisingly different.

This article is part of such dual investigations, where the problem is that of *Frobenius distributions in GL-extensions,* generated by elliptic curves over number fields and by Drinfeld modules over function fields. In particular, the article focuses on the problem of determining the *distribution of the first elementary divisor* of the reduction modulo a prime of a generic Drinfeld module, as the prime varies. Our main result is analogous to a generalization of a result of J.-P. Serre [Se], proven in [CoMu] and [Co3], for the reductions modulo primes of an elliptic curve over $\mathbb{Q}$. The techniques used in proving our main result lead to further applications, such as to Drinfeld module analogues of a result of W. Duke [Du] and of a recent result of T. Freiberg and P. Kurlberg [FrKu], as we now explain.

Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$, and for a prime p of good reduction, let $E_p/\mathbb{F}_p$ be the reduction of E modulo p. By the theory of torsion points of elliptic curves, there exist uniquely determined positive integers $d_{1,p}(E), d_{2,p}(E)$ such that

$$E_p(\mathbb{F}_p) \simeq_{\mathbb{Z}} \mathbb{Z}/d_{1,p}(E)\mathbb{Z} \times \mathbb{Z}/d_{2,p}(E)\mathbb{Z}$$

and

$$d_{1,p}(E)|d_{2,p}(E).$$

In the theory of $\mathbb{Z}$-modules, the integers $d_{1,p}(E), d_{2,p}(E)$ are called the **elementary divisors** of $E_p(\mathbb{F}_p)$, with the largest of them, $d_2 = d_{2,p}(E)$, called the **exponent**, having the property that $d_2 x = 0$ for all $x \in E_p(\mathbb{F}_p)$ (see the general definition in [La, p. 149]).

The study of the growth of $d_{2,p}(E)$, as the prime p varies and $E/\mathbb{Q}$ is fixed, was initiated by R. Schoof [Sc], who showed that, if $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$, then

$$d_{2,p}(E) \gg \frac{\log p}{(\log\log p)^2}\sqrt{p}. \tag{1}$$

W. Duke [Du] improved this bound substantially, but in an "almost all" sense. To be precise, Duke showed that, given any positive function f with $\lim_{x\to\infty} f(x) = \infty$, then, as $x \to \infty$,

$$\#\left\{p \le x : d_{2,p}(E) > \frac{p}{f(p)}\right\} \sim \pi(x), \tag{2}$$

unconditionally if $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \not\simeq \mathbb{Z}$, and conditionally upon the Generalized Riemann Hypothesis (GRH) if $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$; here, $\pi(x)$ denotes the number of primes $p \leq x$. By the "Riemann hypothesis for curves over finite fields" (Hasse's bound in this case), the numerator p in the growth $\frac{p}{f(p)}$ of $d_{2,p}(E)$ above is nothing but the order of magnitude of $\#E_p(\mathbb{F}_p)$. Thus, roughly, Duke's result says that, for almost all p, the exponent of $E_p(\mathbb{F}_p)$ is almost as large as the order of $E_p(\mathbb{F}_p)$. This behaviour is also confirmed by a recent result of T. Freiberg and P. Kurlberg [FrKu] (see also the follow up papers by S. Kim [Ki] and J. Wu [Wu]), in the following sense. Under the same assumptions as Duke's, Freiberg and Kurlberg showed that, as $x \to \infty$,

$$\frac{1}{\pi(x)} \sum_{p \leq x} d_{2,p}(E) \sim c(E)x \tag{3}$$

for some explicit constant $c(E) \in (0,1)$, depending on E.

The proofs of (2) and (3) reduce to the analysis of sums of the form

$$\sum_{y<d<z} \#\{p \leq x : d | d_{1,p}(E)\}$$

for suitable parameters $y = y(x), z = z(x)$. In particular, they reduce to an understanding of the first elementary divisor $d_{1,p}(E)$.

The study of $d_{1,p}(E)$, as the prime p varies and $E/\mathbb{Q}$ is fixed, has been carried out for over four decades and precedes the study of $d_{2,p}(E)$. Most notably, J.-P. Serre [Se] studied the distribution of the primes p for which $d_{1,p}(E) = 1$ in analogy to the study of the Artin primitive root conjecture, while M. R. Murty [Mu] and, later, the first author of this paper, refined and strengthened Serre's result, proving the following (see [Co1], [Co2], [CoMu], and [Co3]): for any $d \in \mathbb{N}$, there exists an explicit constant $\delta_{E,\mathbb{Q}}(d) \geq 0$ such that, as $x \to \infty$,

$$\#\{p \leq x : d_{1,p}(E) = d\} \sim \delta_{E,\mathbb{Q}}(d)\pi(x), \tag{4}$$

unconditionally if $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \not\simeq \mathbb{Z}$, and conditionally upon GRH if $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$. Under GRH, Cojocaru and Murty [CoMu] (see also [Co3]) showed that the error term in this asymptotic is $\mathrm{O}_{E,d}\left(x^{\frac{3}{4}}(\log x)^{\frac{1}{2}}\right)$ if $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \not\simeq \mathbb{Z}$, and $\mathrm{O}_{E,d}\left(x^{\frac{5}{6}}(\log x)^{\frac{2}{3}}\right)$ if $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$.

When considering the function field analogue of these problems, we are naturally led to Drinfeld modules. Indeed, the role played by *elliptic curves* over $\mathbb{Q}$ in number field arithmetic is similar to the one played by *rank 2 Drinfeld modules* over $\mathbb{F}_q(T)$ in function field arithmetic. Drinfeld modules also come in higher generalities, for example in higher ranks, and, as such, when suitable, we may focus on Drinfeld modules of *arbitrary* rank.

To state our main results, we fix the following: q a prime power; $A := \mathbb{F}_q[T]$; $k := \mathbb{F}_q(T)$; $K \supseteq k$ a finite field extension; $\psi : A \longrightarrow K\{\tau\}$ a generic Drinfeld A-module over K, of rank $r \geq 2$. Here, $\tau : x \mapsto x^q$ is the q-th power Frobenius automorphism and $K\{\tau\}$ is the skew-symmetric polynomial ring in τ over K (we will review definitions and basic properties in Sections 2 and 3).

By classical theory, all but finitely many of the primes $\wp$ of K are of good reduction for ψ. We denote by $\mathcal{P}_\psi$ the collection of these primes, and for each $\wp \in \mathcal{P}_\psi$, we consider the residue field $\mathbb{F}_\wp$ at $\wp$ and the A-module structure on $\mathbb{F}_\wp$, denoted $\psi(\mathbb{F}_\wp)$, defined by the reduction $\psi \otimes \wp : A \longrightarrow \mathbb{F}_\wp\{\tau\}$ of ψ modulo $\wp$.

By the theory of torsion points for Drinfeld modules and that of finitely generated modules over a PID, there exist uniquely determined monic polynomials $d_{1,\wp}(\psi), \ldots, d_{r,\wp}(\psi) \in A$ such that

$$\psi(\mathbb{F}_\wp) \simeq_A A/d_{1,\wp}(\psi)A \times \ldots \times A/d_{r,\wp}(\psi)A \tag{5}$$

and

$$d_{1,\wp}(\psi)| \ldots |d_{r,\wp}(\psi).$$

The polynomials $d_{1,\wp}(\psi), \ldots, d_{r,\wp}(\psi)$ are the **elementary divisors** of the A-module $\psi(\mathbb{F}_\wp)$, with the largest of them, $d_r = d_{r,\wp}(\psi)$, the **exponent**, having the property that $d_r x = 0$ for all $x \in \psi(\mathbb{F}_\wp)$. Here, $d_r x := (\psi \otimes \mathbb{F}_\wp)(d_r)(x)$.

Associated to this setting, we introduce the following additional notation. We let $\mathbb{F}_K$ denote the constant field of K and $c_K := [\mathbb{F}_K : \mathbb{F}_q]$; thus $\mathbb{F}_K = \mathbb{F}_{q^{c_K}}$. For a non-zero $a \in A$, we let $|a|_\infty := q^{\deg a}$, where $\deg a$ is the degree of a as a polynomial in T. For a prime $\wp$ of K, we let $\deg_K \wp := [\mathbb{F}_\wp : \mathbb{F}_K]$ and $|\wp|_\infty := q^{c_K \deg_K \wp}$. We set

$$\pi_K(x) := \#\{\wp \text{ prime of } K : \deg_K \wp = x\}$$

and recall the effective Prime Number Theorem for K:

$$\pi_K(x) = \frac{q^{c_K x}}{x} + \mathrm{O}_K\left(\frac{q^{\frac{c_K x}{2}}}{x}\right). \tag{6}$$

The first main result of the paper is:

Theorem 1. *Let q be a prime power, $A := \mathbb{F}_q[T]$, $k := \mathbb{F}_q(T)$, and K/k a finite field extension. Let $\psi : A \longrightarrow K\{\tau\}$ be a generic Drinfeld A-module over K, of rank $r \geq 2$. Let $d \in A$ be monic. Then, as $x \to \infty$,*

$$\#\{\wp \in \mathcal{P}_\psi : \deg_K \wp = x, d_{1,\wp}(\psi) = d\} \sim \pi_K(x) \sum_{\substack{m \in A \\ m \text{ monic}}} \frac{\mu_A(m) c_{md}(x)}{[K(\psi[md]) : K]}, \tag{7}$$

where $\mu_A(\cdot)$ is the Möbius function on A, $K(\psi[md])$ is the md-division field of ψ, and

$$c_{md}(x) := \begin{cases} [K(\psi[md]) : \cap \overline{\mathbb{F}}_K : \mathbb{F}_K] & \text{if} \quad [K(\psi[md]) \cap \overline{\mathbb{F}}_K : \mathbb{F}_K] \mid x, \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, the Dirichlet density of the set

$$\{\wp \in \mathcal{P}_\psi : d_{1,\wp}(\psi) = d\}$$

exists and is given by

$$\delta_{\psi,K}(d) := \sum_{\substack{m \in A \\ m \text{ monic}}} \frac{\mu_A(m)}{[K(\psi[md]) : K]}. \tag{8}$$

This is a large generalization of a result proven independently in [KuLi].

The essence of the proof of this theorem may be summarized as a Chebotarev Density Theorem for *infinitely many* Galois extensions generated by the generic Drinfeld module ψ:

Theorem 2. *Let q be a prime power, $A := \mathbb{F}_q[T]$, $k := \mathbb{F}_q(T)$, and K/k a finite field extension. Let $\psi : A \longrightarrow K\{\tau\}$ be a generic Drinfeld A-module over K, of rank $r \geq 2$. Then, as $x \to \infty$,*

$$\sum_{\substack{m \in A \\ m \text{ monic}}} \#\{\wp \in \mathcal{P}_\psi : \deg_K \wp = x, \wp \text{ splits completely in } K(\psi[m])\} \sim \pi_K(x) \sum_{\substack{m \in A \\ \text{monic}}} \frac{c_m(x)}{[K(\psi[m]) : K]},$$

with notation as in Theorem 1.

As a consequence of the techniques used in proving Theorems 1 and 2, we obtain the following analogues of the results of [Du] and [FrKu] in the case of a rank 2 generic Drinfeld module over K:

Theorem 3. *Let q be a prime power, $A := \mathbb{F}_q[T]$, $k := \mathbb{F}_q(T)$, and K/k a finite field extension. Let $\psi : A \longrightarrow K\{\tau\}$ be a generic Drinfeld A-module over K, of rank 2.*

(i) *Let $f : (0, \infty) \longrightarrow (0, \infty)$ be such that $\lim_{x \to \infty} f(x) = \infty$ and $f(x) < \frac{x}{2}\ \forall x$. Then, as $x \to \infty$,*

$$\#\left\{\wp \in \mathcal{P}_\psi : \deg_K \wp = x, |d_{2,\wp}(\psi)|_\infty > \frac{|\wp|_\infty}{q^{c_K f(x)}}\right\} \sim \pi_K(x).$$

Moreover, if there exists $0 < \theta < 1$ such that $f(x) \leq \frac{\theta x}{2}\ \ \forall x$, then the Dirichlet density of the set

$$\left\{\wp \in \mathcal{P}_\psi : |d_{2,\wp}(\psi)|_\infty > \frac{|\wp|_\infty}{q^{c_K f(\deg_K \wp)}}\right\}$$

exists and equals 1.

(ii) *There exists an explicit constant $c(\psi, K)$, depending on ψ and K, such that, as $x \to \infty$,*

$$\frac{1}{\pi_K(x)} \sum_{\substack{\wp \in \mathcal{P}_\psi \\ \deg_K \wp = x}} |d_{2,\wp}(\psi)|_\infty \sim c(\psi, K) q^{c_K x}.$$

2. Notation and basic facts

Throughout the paper, we will use the following notation and basic results.

2.1. $\mathbb{N}, \mathbb{R}, \mathbb{C}$ **notation.** We use $\mathbb{N}$ for the set of natural numbers $\{1, 2, 3, \ldots\}$, and $\mathbb{R}$, $\mathbb{C}$ for the sets of real, respectively complex numbers.

2.2. $\mathrm{O}, \ll, \mathrm{o}, \sim$ **notation.** For two functions $f, g : D \longrightarrow \mathbb{R}$, with $D \subseteq \mathbb{C}$ and g positive, we write $f(x) = \mathrm{O}(g(x))$ or $f(x) \ll g(x)$ if there is a positive constant C such that $|f(x)| \leq Cg(x)$ for all $x \in D$. If C depends on another specified object C', we write $f(x) = \mathrm{O}_{C'}(g(x))$ or $f(x) \ll_{C'} g(x)$. We write $f(x) = \mathrm{o}(g(x))$ if $\lim_{x \to \infty} \frac{f(x)}{g(x)} = 0$, and $f(x) \sim g(x)$ if $\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1$ (whenever the limits exist).

2.3. **Elementary arithmetic.** We let q be a prime power, fixed throughout the paper. Our implied O-constants may depend on q, without any additional specification.

We denote by $\mathbb{F}_q$ the finite field with q elements, by $\mathbb{F}_q^*$ its group of units, by $\overline{\mathbb{F}}_q$ an algebraic closure, and by $\tau : x \mapsto x^q$ the q-th power Frobenius automorphism.

As in Section 1, we denote by $A := \mathbb{F}_q[T]$ the polynomial ring over $\mathbb{F}_q$ and by $k := \mathbb{F}_q(T) = \mathrm{Quot}(A)$ its field of fractions; we denote by $A^{(1)}$ the set of monic polynomials in A.

We recall that A is a Euclidean domain, hence the greatest common divisor, denoted gcd, and the least common multiple, denoted lcm, exist in A. We recall that $\frac{1}{T}$ plays the role of the "prime at infinity" of k, while the "finite primes" of k are identified with monic irreducible polynomials of A. We will simply refer to the latter as the **primes of** k.

We denote the monic irreducible elements of A by p or ℓ. We denote the primes of k by $\mathfrak{p} = pA$, with $p \in A^{(1)}$, or by $\mathfrak{l} = \ell A$, with $\ell \in A^{(1)}$. For such primes, we denote their residue fields by $\mathbb{F}_\mathfrak{p}$, $\mathbb{F}_\mathfrak{l}$, and the completions of A, respectively of k, by $A_\mathfrak{p}$, $A_\mathfrak{l}$, and $k_\mathfrak{p}$, $k_\mathfrak{l}$.

For $a \in A$, we use the standard notation:

- $\deg a$ for the degree of $a \neq 0$ as a polynomial in T, and $\deg 0 := -\infty$;
- $|a|_\infty := q^{\deg a}$ if $a \neq 0$, and $|0|_\infty := 0$;
- $\mathrm{sgn}(a) \in \mathbb{F}_q$ for the leading coefficient of a;
- $\mu_A(a)$ for the Möbius function of a on A; that is, using the notation $a = \mathrm{sgn}(a) \cdot p_1^{e_1} \dots p_t^{e_t}$ for the prime decomposition of $a \in \mathbb{F}_q[T]\backslash\{0\}$, we have

$$\mu_A(a) := \begin{cases} 1 & \text{if } a \in \mathbb{F}_q^*, \\ (-1)^t & \text{if } a \in \mathbb{F}_q[T]\backslash\{0\} \text{ and } e_1 = e_2 = \ldots = e_t = 1, \\ 0 & \text{otherwise;} \end{cases}$$

- $(A/aA)^*$ for the group of units of A/aA;
- $\phi_A(a)$ for the Euler function of a on A; that is,

$$\begin{aligned} \phi_A(a) &= \#(A/aA)^* \\ &= \#\{a' \in A\backslash\{0\} : \deg a' \leq \deg a, \gcd\{a, a'\} = 1\} \\ &= |a|_\infty \prod_{\substack{p \in A^{(1)} \\ p \mid a}} \left(1 - \frac{1}{|p|_\infty}\right); \end{aligned}$$

- $\mathrm{GL}_r(A/aA) := \{(a_{ij})_{1 \leq i,j \leq r} : a_{ij} \in A/aA, \det(a_{ij})_{i,j} \in (A/aA)^*\}$.

We record below a few arithmetic results needed in the proofs of our main theorems.

Lemma 4. *Let $y \in \mathbb{N}$. Then:*

(i) $$\sum_{\substack{a \in A^{(1)} \\ 0 \leq \deg a \leq y}} 1 = \frac{q^{y+1} - 1}{q - 1};$$

(ii) $$\sum_{\substack{a\in A^{(1)}\\ 0\le \deg a\le y}} \deg a \le y\frac{q^{y+1}-1}{q-1}.$$

Proof. Elementary. □

Lemma 5. *Let $y\in\mathbb{N}\backslash\{1,2\}$ and let $\alpha>1$. Then:*

(i) $$\sum_{\substack{a\in A\\ \deg a>y}} \frac{1}{q^{\alpha\deg a}} = \frac{q}{\left(1-\frac{1}{q^{\alpha-1}}\right)q^{(\alpha-1)(y+1)}};$$

(ii) $$\sum_{\substack{a\in A\\ \deg a>y}} \frac{\log\deg a}{q^{\alpha\deg a}} \le \frac{\log y}{(\alpha-1)q^{(\alpha-1)y}\log q} + \frac{1}{y(\alpha-1)^2q^{(\alpha-1)y}(\log q)^2}.$$

Proof. Elementary. □

Lemma 6. *Let $a\in A$. Then*

$$\sum_{\substack{d\in A\\ d\mid a}} \mu_A(d) = \begin{cases} q-1 & \text{if } a\in\mathbb{F}_q^*,\\ 0 & \text{otherwise.}\end{cases}$$

Proof. If $a\in\mathbb{F}_q^*$, then

$$\sum_{\substack{d\in A\\ d\mid a}} \mu_A(d) = \sum_{d\in\mathbb{F}_q^*} 1 = q-1.$$

If $a\notin\mathbb{F}_q^*$, let

$$a = \operatorname{sgn}(a)\cdot p_1^{e_1}\dots p_t^{e_t}$$

be the prime factorization of a and let

$$\operatorname{rad}(a) := \operatorname{sgn}(a)\cdot p_1\dots p_t$$

be the radical of a. Then

$$\sum_{\substack{d\in A\\ d\mid a}} \mu_A(d) = \sum_{\substack{d\in A\\ d\mid \operatorname{rad}(a)}} \mu_A(d).$$

Note that, if $\mathbb{F}_q^*=\langle u\rangle$, then the divisors $d\mid\operatorname{rad}(a)$ are of the form: u^α for some $1\le\alpha\le q-1$; or $u^\alpha p_i$ for some $1\le\alpha\le q-1$ and some $1\le i\le t$; or $u^\alpha p_{i_1}p_{i_2}$ for some $1\le\alpha\le q-1$ and some $1\le i_1<i_2\le t$, and so on. For the first, there are $(q-1)\binom{t}{0}$ possibilities, for the second there are $(q-1)\binom{t}{1}$ possibilities, for the third there are $(q-1)\binom{t}{2}$ possibilities, and so on. In summary, we have

$$\sum_{\substack{d\in A\\ d\mid\operatorname{rad}(a)}} \mu_A(d) = \sum_{0\le i\le t}(q-1)\binom{t}{i}(-1)^i = (q-1)(1-1)^t = 0.$$

This completes the proof. □

Lemma 7. *Let $d\in A$. Then*

$$\frac{1}{|d|_\infty} = \frac{1}{(q-1)^2}\sum_{\substack{d_1,d_2\in A\\ d_1d_2\mid d}} \frac{\mu_A(d_1)}{|d_2|_\infty}.$$

Proof. We have

$$\begin{aligned}
\frac{1}{(q-1)^2}\sum_{\substack{d_1,d_2\in A\\ d_1d_2|d}}\frac{\mu_A(d_1)}{|d_2|_\infty} &= \frac{1}{(q-1)^2}\sum_{\substack{a\in A\\ a|d}}\sum_{\substack{n\in A\\ n|a}}\mu_A\left(\frac{a}{n}\right)\frac{1}{|n|_\infty}\\
&= \frac{1}{(q-1)^2}\sum_{\substack{n\in A\\ n|d}}\frac{1}{|n|_\infty}\sum_{\substack{m\in A\\ m|\frac{d}{n}}}\mu_A(m)\\
&= \frac{1}{(q-1)^2}\sum_{\substack{n\in A\\ n|d}}\frac{1}{|n|_\infty}(q-1)\\
&= \frac{1}{(q-1)|d|_\infty}\sum_{u\in\mathbb{F}_q^*}1\\
&= \frac{1}{|d|_\infty},
\end{aligned}$$

by also using Lemma 6. □

Lemma 8. *Let $d\in A^{(1)}$. Then*

$$\sum_{\substack{m,n\in A^{(1)}\\ mn=d}}\frac{\mu_A(m)}{|n|_\infty}=\frac{(-1)^{\omega(d)}\phi_A(rad\,(a))}{|d|_\infty},$$

where $\omega(d)$ is the number of all monic prime divisors of d (counted with multiplicities) and rad (d) is the radical of d.

Proof. By multiplicativity, we have

$$\sum_{\substack{m,n\in A^{(1)}\\ mn=d}}\frac{\mu_A(m)}{|n|_\infty}=\prod_{\substack{p\in A^{(1)}\\ p^t||d}}\sum_{\substack{n\in A^{(1)}\\ n|p^t}}\frac{\mu_A\left(\frac{p^t}{n}\right)}{|n|_\infty}=\prod_{\substack{p\in A^{(1)}\\ p^t||d}}\frac{1-|p|_\infty}{|p|_\infty^t}=\frac{(-1)^{\omega(d)}\phi_A(\text{rad }(a))}{|d|_\infty}.$$

□

2.4. ***A*-modules.** For A-modules M_1, M_2, we write $M_1\simeq_A M_2$ to mean that M_1, M_2 are isomorphic over A, and $M_1\leq_A M_2$ to mean that M_1 is an A-submodule of M_2.

For a non-zero finite A-module M, we let $\chi(M)$ be its **Euler-Poincaré characteristic**, defined as the ideal of A uniquely determined by the conditions:

(i) if $M\simeq_A A/\mathfrak{p}$ for a prime ideal $\mathfrak{p}$ of A, then $\chi(M):=\mathfrak{p}$;

(ii) if $0\to M_1\to M\to M_2\to 0$ is an exact sequence of A-modules, then $\chi(M)=\chi(M_1)\chi(M_2)$.

We let $|\chi(M)|_\infty:=|m|_\infty$ for some generator $m\in A$ of $\chi(M)$.

2.5. ***A*-fields.** We reserve the notation (L,δ) for ***A*-fields**, that is, pairs consisting of a field $L\supseteq\mathbb{F}_q$ and an $\mathbb{F}_q$-algebra homomorphism $\delta: A\longrightarrow L$. We recall that the kernel of δ is called the ***A*-characteristic of** L; in particular, if $\operatorname{Ker}\delta=(0)$, L is said to have **generic** ***A*-characteristic**, and if $\operatorname{Ker}\delta\neq(0)$, L is said to have **finite** ***A*-characteristic**.

We denote by $\overline{L}$ an algebraic closure of L, by L^{sep} the separable closure of L in $\overline{L}$, and by $G_L := \mathrm{Gal}(L^{\mathrm{sep}}/L)$ the absolute Galois group of L. We also denote by $L\{\tau\}$ the **skew-symmetric polynomial ring in τ over L**, that is,

$$L\{\tau\} := \left\{ \sum_{0 \le i \le n} c_i \tau^i : c_i \in L \ \forall\, 0 \le i \le n, n \in \mathbb{N} \cup \{0\} \right\},$$

with the multiplication rule

$$\tau c = c^q \tau \ \forall c \in L.$$

For an element $f \in L\{\tau\}$, we denote by $\deg_\tau(f)$ its degree as a polynomial in τ. We recall that $L\{\tau\}$ is isomorphic to the $\mathbb{F}_q$-endomorphism ring $\mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_a/L)$ of the additive group scheme $\mathbb{G}_a$ over L.

2.6. **Finite field extensions of k.** We reserve the notation K for a finite field extension of k of genus g_K. We denote by $\overline{K}$ an algebraic closure of K, by K^{sep} the separable closure of K in $\overline{K}$, by $K\{\tau\}$ the skew-symmetric polynomial ring over K, by $\mathbb{F}_K$ the constant field of K (that is, $\mathbb{F}_K = K \cap \overline{\mathbb{F}}_q$), and by $\overline{\mathbb{F}}_K$ an algebraic closure of $\mathbb{F}_K$. We set $c_K := [\mathbb{F}_K : \mathbb{F}_q]$.

By a **prime of K** we mean a discrete valuation ring $\mathcal{O}$ with maximal ideal $\mathcal{M}$ such that $\mathbb{F}_K \subseteq \mathcal{O}$ and the quotient field $\mathrm{Quot}(\mathcal{O})$ of $\mathcal{O}$ equals K. In particular, for a prime $\wp$ of K, we denote by $(\mathcal{O}_\wp, \mathcal{M}_\wp)$ the associated discrete valuation ring, by $\mathbb{F}_\wp := \mathcal{O}_\wp/\mathcal{M}_\wp$ the associated residue field, by $\deg_K \wp := [\mathbb{F}_\wp : \mathbb{F}_K]$ the degree of $\wp$ in K, by $\overline{\mathbb{F}}_\wp$ an algebraic closure of $\mathbb{F}_\wp$, and by $\mathbb{F}_\wp^{\mathrm{sep}}$ the separable closure of $\mathbb{F}_\wp$ in $\overline{\mathbb{F}}_\wp$. We make the convention that $\wp$ satisfies $\wp \cap A = pA$ for some $p \in A^{(1)}$ irreducible, and we denote this ideal by $\mathfrak{p}$. We set $m_\wp := [\mathbb{F}_\wp : A/\mathfrak{p}]$ and record the diagram:

$$\begin{array}{ccccc} & & \mathbb{F}_\wp := \mathcal{O}_\wp/\mathcal{M}_\wp & & \\ & \overset{\deg_K \wp}{\nearrow} & & \overset{m_\wp}{\nwarrow} & \\ \mathbb{F}_K := \mathbb{F}_{q^{c_K}} & & & & \mathbb{F}_\mathfrak{p} := A/\mathfrak{p} = \mathbb{F}_{q^{\deg p}} \\ & \underset{c_K}{\searrow} & & \underset{\deg p}{\swarrow} & \\ & & \mathbb{F}_q & & \end{array} \tag{9}$$

Hence the relationship between the $|\cdot|_\infty$-norm of a prime $\wp$ of K and its associated prime $\mathfrak{p} = pA$ in k is

$$|\wp|_\infty = |p|_\infty^{m_\wp}.$$

Finally, for a finite Galois extension K' of K, we write $\sigma_\wp$ for the Artin symbol ("the Frobenius") at $\wp$ in K'/K.

3. Drinfeld modules

3.1. **Basic definitions.** Let (L, δ) be an A-field. A **Drinfeld A-module over L** is an $\mathbb{F}_q$-algebra homomorphism

$$\psi : A \longrightarrow L\{\tau\}$$

$$a \longmapsto \psi_a$$

such that:

(1) for all $a \in A$, $D(\psi_a) = \delta(a)$, where $D : L\{\tau\} \longrightarrow L$, $D\left(\sum_{0 \leq i \leq n} c_i \tau^i\right) = c_0$ is the differentiation with respect to x map;

(2) $\operatorname{Im} \psi \not\subseteq L$.

A homomorphism ψ as above induces a nontrivial A-module structure on L, or, more generally, on any L-algebra Ω; we denote this structure by $\psi(\Omega)$.

Associated to a Drinfeld A-module ψ over L we have two important invariants, called the rank and the height. We define the **rank** of ψ as the unique positive integer r such that

$$\deg_\tau(\psi_a) = r \deg a \ \ \forall a \in A.$$

If L has generic A-characteristic, we define the **height** of ψ as zero. If L is of finite A-characteristic $\mathfrak{p} = pA$, we define the **height** of ψ as the unique positive integer h such that

$$\min\{0 \leq i \leq r \deg a : c_{i,a}(\psi) \neq 0\} = h \operatorname{ord}_{\mathfrak{p}}(a) \deg p \ \ \forall a \in A, a \neq 0,$$

where

$$\psi_a = \sum_{0 \leq i \leq r \deg a} c_{i,a}(\psi) \tau^i$$

and $\operatorname{ord}_{\mathfrak{p}}(a) := t$ with p^t the highest power of p dividing a.

For the purpose of this paper, the rank and the height are particularly relevant in determining the structure (5) of the reductions modulo primes of a Drinfeld A-module in generic characteristic.

3.2. **Endomorphism rings.** Let (L, δ) be an A-field. Given $\psi, \psi' : A \longrightarrow L\{\tau\}$ Drinfeld A-modules over L, a **morphism from ψ to ψ' over** L is an element $f \in L\{\tau\}$ such that

$$f\psi_a = \psi'_a f \ \ \forall a \in A.$$

An **isomorphism from ψ to ψ' over** L is an element $f \in L^*$ such that $f\psi_a = \psi'_a f \ \ \forall a \in A$. An **isogeny from ψ to ψ' over** L is a non-zero morphism as above. Finally, $\operatorname{End}_L(\psi)$ and $\operatorname{End}_{\overline{L}}(\psi)$ are the rings of endomorphisms of ψ over L and over $\overline{L}$, respectively.

We remark that

$$\psi(A) \subseteq \operatorname{End}_L(\psi) \subseteq \operatorname{End}_{\overline{L}}(\psi)$$

and that isogenous Drinfeld modules have the same rank and height.

For ease of notation, we shall henceforth denote the category of Drinfeld A-modules over L by

$$\operatorname{Drin}_A(L).$$

Remark 9. The category $\mathrm{Drin}_A(L)$ of Drinfeld A-modules over L may be defined in greater generality. Indeed, we may fix an arbitrary function field $\mathscr{K}$ and a prime ∞ of $\mathscr{K}$. We then take $\mathscr{A}$ as the ring of functions on $\mathscr{K}$ regular away from ∞ and define the category $\mathrm{Drin}_{\mathscr{A}}(\mathscr{L})$ of Drinfeld $\mathscr{A}$-modules over $\mathscr{A}$-fields $\mathscr{L}$ exactly as we did above.

The endomorphism rings introduced here have important properties, such as:

Theorem 10. *(* [Go, Prop. 4.7.6 p. 80, Theorem 4.7.8 p. 81, Prop. 4.7. 17 p. 84], [Th, Theorem 2.7.2, p. 50]*)*

Let (L,δ) be an A-field with generic A-characteristic. Let $\psi \in \mathrm{Drin}_A(L)$ be of rank $r \geq 1$. Then:

(i) $\mathrm{End}_{\overline{L}}(\psi)$ *is commutative;*

(ii) $\mathrm{End}_{\overline{L}}(\psi)$ *is a finitely generated projective A-module of rank at most r;*

(iii) *if we denote by*

$$k' := \mathrm{End}_{\overline{L}}(\psi) \otimes_A k,$$

then k' is a finite field extension of k satisfying $[k' : k] \leq r$.

3.3. **Division points.** Let (L,δ) be an A-field and let $\psi \in \mathrm{Drin}_A(L)$. Let $a \in A\backslash\mathbb{F}_q$. We define the **$a$-division module of** ψ by

$$\psi[a] := \left\{\lambda \in \overline{L} : \psi_a(\lambda) = 0\right\}.$$

When $a = \ell$ is irreducible, we define the **ℓ^∞-division module of** ψ by

$$\psi\left[\ell^\infty\right] := \bigcup_{n\geq 1} \psi\left[\ell^n\right].$$

Note that $\psi[a]$ is a torsion A-module via ψ. As we recall below, its A-module structure is well determined by a and ψ.

Theorem 11. [Ro, Theorem 13.1 p. 221]

Let (L,δ) be an A-field with A-characteristic $\mathfrak{p}$ (possibly zero). Let $\psi \in \mathrm{Drin}_A(L)$ be of rank $r \geq 1$ and height h. Let $\mathfrak{l} \neq \mathfrak{p}$ be a non-zero prime ideal of A with $\mathfrak{l} = \ell A$, and let $e \geq 1$ be any integer. Then

$$\psi[\ell^e] \simeq_A (A/\ell^e A)^r.$$

If $\mathfrak{p} = pA$ is non-zero, then

$$\psi[p^e] \simeq_A (A/p^e A)^{r-h}.$$

Corollary 12. *Let (L,δ) be an A-field with A-characteristic $\mathfrak{p}$ (possibly zero). Let $\psi \in \mathrm{Drin}_A(L)$ be of rank $r \geq 1$ and height h. Let $a \in A\backslash\mathbb{F}_q$ and write the ideal aA (uniquely) as the product of ideals $\mathfrak{a}_1, \mathfrak{a}_2$ of A such that $\mathfrak{a}_1$ is relatively prime to $\mathfrak{p}$ and $\mathfrak{a}_2$ is composed of prime divisors of $\mathfrak{p}$. Then*

$$\psi[a] \simeq_A (A/\mathfrak{a}_1)^r \oplus (A/\mathfrak{a}_2)^{r-h} \leq_A (A/\mathfrak{a})^r.$$

Remark 13. Theorem 11 and Corollary 12 hold in greater generality. In particular, the results hold for a Drinfeld module $\psi \in \mathrm{Drin}_{\mathscr{A}}(\mathscr{L})$, where $\mathscr{A}$ is the ring of functions on an arbitrary function field $\mathscr{K}$ which are regular away from some fixed prime in $\mathscr{K}$, and where $\mathscr{L}$ is any $\mathscr{A}$-field.

The absolute Galois group of L acts on each $\psi[a]$ and this action leads to the Galois extensions $L(\psi[a])$ of L, to be discussed in Section 3.6.

3.4. **Reductions modulo primes.** Let (L, δ) be an A-field and let $\psi \in \mathrm{Drin}_A(L)$ be of rank $r \geq 1$. Let $\wp$ be a prime of L.

We say that ψ **has integral coefficients at** $\wp$ if:

(1) $\psi_a \in \mathcal{O}_\wp\{\tau\} \ \ \forall a \in A$;

(2) $\psi \otimes \mathbb{F}_\wp : A \longrightarrow \mathbb{F}_\wp\{\wp\}$, defined by $a \mapsto \psi_a (\mathrm{mod}\, \wp)$, is a Drinfeld A-module over $\mathbb{F}_\wp$ (of some rank $0 < r_1 \leq r$).

In this case, we also say that $\psi \otimes \mathbb{F}_\wp$ is the **reduction of** ψ **modulo** $\wp$.

We say that ψ **has good reduction at** $\wp$ if there exists $\psi' \in \mathrm{Drin}_A(L)$ such that:

(1) $\psi' \simeq_K \psi$;

(2) ψ' has integral coefficients at $\wp$;

(3) $\psi' \otimes \mathbb{F}_\wp$ has rank r.

For the remainder of this subsection, we assume that $L = K$ is a finite field extension of k and that $\psi \in \mathrm{Drin}_A(K)$ has generic characteristic. There are only finitely many primes of K which are *not* of good reduction for $\psi \in \mathrm{Drin}_A(K)$. As in Section 1, we let $\mathcal{P}_\psi$ denote the set of (finite) primes of K of good reduction for ψ.

Note that, for a prime $\wp \in \mathcal{P}_\psi$, Corollary 12 gives the structure (5) of the A-module $\psi(\mathbb{F}_\wp)$. Indeed, $\psi(\mathbb{F}_\wp)$ is a finite A-module, and since A is a PID, there exist unique polynomials $d_{1,\wp}(\psi), d_{2,\wp}(\psi), \ldots, d_{s,\wp}(\psi) \in A^{(1)}$ such that

$$\psi(\mathbb{F}_\wp) \simeq_A A/d_{1,\wp}(\psi)A \times \ldots \times A/d_{s,\wp}(\psi)A,$$

with $d_{i,\wp}(\psi) | d_{i+1,\wp}(\psi)$ for all $i = 1, \ldots, s-1$. That $s = r$ follows from the fact that $\psi(\mathbb{F}_\wp)$ is a torsion module, and hence, by Corollary 12, from the existence of some $a \in A \backslash \mathbb{F}_q$ such that $\psi(\mathbb{F}_\wp) \leq_A \psi[a] \leq_A (A/aA)^r$.

The following analogue of the criterion of Néron-Ogg-Shafarevich for elliptic curves holds:

Theorem 14. [Tak, Theorem 1, p. 477]
Let K be a finite extension of k. Let $\psi \in \mathrm{Drin}_A(K)$ be of generic characteristic. Let $\wp$ be a prime of K and let $\mathfrak{l} = \ell A$ be a prime ideal different from $\mathfrak{p} := \wp \cap A$. Then ψ has good reduction at $\wp$ if and only if the Galois module $\psi[\ell^\infty]$ is unramified at $\wp$. Moreover, if ψ has rank 1, then $\psi[\ell^\infty]$ is totally ramified at $\mathfrak{l}$.

Note that while the last assertion of the theorem is not stated explicitly in [Tak, Theorem 1, p. 477], it can be derived from its proof.

Remark 15. The notion of good reduction can be introduced for a general $\psi \in \mathrm{Drin}_{\mathscr{A}}(\mathscr{L})$, where $\mathscr{A}$ is the ring of functions on an arbitrary function field $\mathscr{K}$ which are regular away from some fixed prime in $\mathscr{K}$, and $\mathscr{L}$ is a generic $\mathscr{A}$-field. Theorem 14 holds in this general setting also.

3.5. **Division fields.** Let K be a finite field extension of k and let $\psi \in \mathrm{Drin}_A(K)$ be of generic characteristic. For $a \in A$, we define the **a-division field of** ψ as $K(\psi[a])$. This is a Galois extension of K which plays a crucial role in our study of the elementary divisors of the reductions of ψ. We denote the genus of $K(\psi[a])$ by g_a and the degree of the constant field of $K(\psi[a])$ over $\mathbb{F}_K$ by c_a, that is,

$$c_a := [K(\psi[a]) \cap \overline{\mathbb{F}}_K : \mathbb{F}_K]. \tag{10}$$

Below are important properties of these division fields.

Proposition 16. [Go, Remark 7.1.9, p. 196]
Let K be a finite field extension of k and let $\psi \in \mathrm{Drin}_A(K)$ be of generic characteristic. Let

$$K_{\psi,tors} := \bigcup_{a \in A \setminus \mathbb{F}_q} K(\psi[a]).$$

Then

$$[K_{\psi,tors} \cap \overline{\mathbb{F}}_K : \mathbb{F}_K] < \infty.$$

In particular, there exists a constant $C(\psi, K) \in \mathbb{N}$, depending on K and ψ, such that, for any $a \in A \setminus \mathbb{F}_q$,

$$c_a \leq C(\psi, K).$$

Proposition 17. [Ga, Corollary 7, p. 248]
Let K be a finite field extension of k and let $\psi \in \mathrm{Drin}_A(K)$ be of generic characteristic. Then there exists a constant $G(\psi, K) \in \mathbb{N}$, depending on K and ψ, such that, for any $a \in A \setminus \mathbb{F}_q$,

$$g_a \leq G(\psi, K) \cdot [K(\psi[a]) : K] \cdot \deg a.$$

3.6. **Galois representations.** We start with a more general setting, as follows. Let $\mathscr{K}$ be a finitely generated field of transcendence degree 1 over $\mathbb{F}_q$, let ∞ be a fixed prime of $\mathscr{K}$, and let $\mathscr{A}$ be the ring of functions on $\mathscr{K}$ regular away from ∞. Let $\mathscr{L}$ be a finitely generated extension of $\mathscr{K}$. Let $\psi \in \mathrm{Drin}_{\mathscr{A}}(\mathscr{L})$ be of rank $r \geq 1$, automatically of generic characteristic.

Using the general notions of division points on Drinfeld modules, for any non-zero prime $\mathfrak{l}$ of $\mathscr{A}$ we define the **$\mathfrak{l}$-adic Tate module of** ψ by

$$T_{\mathfrak{l}}(\psi) := \lim_{\substack{\leftarrow \\ n}} \psi\left[\mathfrak{l}^n\right].$$

This is a free $\mathscr{A}_{\mathfrak{l}}$-module of rank r, where $\mathscr{A}_{\mathfrak{l}}$ denotes the completion of $\mathscr{A}$ at $\mathfrak{l}$. Moreover, this module gives rise to continuous Galois representations

$$\rho_{\mathfrak{l},\psi} : G_{\mathscr{L}} \longrightarrow \mathrm{Aut}_{\mathscr{A}_{\mathfrak{l}}}(T_{\mathfrak{l}}(\psi)) \simeq \mathrm{GL}_r(\mathscr{A}_{\mathfrak{l}}),$$

$$\rho_\psi : G_{\mathscr{L}} \longrightarrow \prod_{\mathfrak{l}\neq\infty} \mathrm{Aut}_{\mathscr{A}_\mathfrak{l}}(T_\mathfrak{l}(\psi)) \simeq \prod_{\mathfrak{l}\neq\infty} \mathrm{GL}_r(\mathscr{A}_\mathfrak{l}) \simeq \mathrm{GL}_r\left(\hat{\mathscr{A}}\right)$$

of the absolute Galois group $G_{\mathscr{L}} := \mathrm{Gal}(\mathscr{L}^{\mathrm{sep}}/\mathscr{L})$ of $\mathscr{L}$. Here, $\hat{\mathscr{A}} := \varprojlim_{\mathfrak{a}} \mathscr{A}/\mathfrak{a}$, where $\mathfrak{a}$ are non-zero ideals of $\mathscr{A}$ ordered by divisibility.

These representations fit into a commutative diagram

$$\begin{array}{ccc} G_{\mathscr{L}} & \xrightarrow{\rho_\psi} & \prod_{\mathfrak{l}\neq\infty} \mathrm{GL}_r(\mathscr{A}_\mathfrak{l}) \\ & \searrow^{\rho_{\mathfrak{l},\psi}} & \downarrow \pi \\ & \searrow^{\bar\rho_{\mathfrak{l}^n,\psi}} & \mathrm{GL}_r(\mathscr{A}_\mathfrak{l}) \\ & & \downarrow \mathrm{mod}\,\mathfrak{l}^n \\ & & \mathrm{GL}_r(\mathscr{A}/\mathfrak{l}^n\mathscr{A}), \end{array}$$

with π denoting the natural projection and $\mathrm{mod}\,\mathfrak{l}^n$ denoting the reduction modulo $\mathfrak{l}^n$ map.

Since the *residual* representation $\bar\rho_{\mathfrak{l}^n,\psi}$ gives rise to an *injective* representation

$$\bar\rho_{\mathfrak{l}^n,\psi} : \mathrm{Gal}(\mathscr{L}(\psi\,[\mathfrak{l}^n])/\mathscr{L}) \hookrightarrow \mathrm{GL}_r(\mathscr{A}/\mathfrak{l}^n\mathscr{A}),$$

we immediately deduce the upper bound

$$[\mathscr{L}(\psi\,[\mathfrak{l}^n]) : \mathscr{L}] \leq \#\,\mathrm{GL}_r(\mathscr{A}/\mathfrak{l}^n\mathscr{A}). \tag{11}$$

This may be better understood using:

Lemma 18. *Let $\mathscr{A}$ be a Dedekind domain whose field of fractions is a global field $\mathscr{K}$. Let $\mathfrak{a}$ be a non-zero ideal of $\mathscr{A}$. Define*

$$|\mathfrak{a}| := \#(\mathscr{A}/\mathfrak{a}).$$

Then, for any $r \in \mathbb{N}$, we have

$$\begin{aligned} \#\,\mathrm{GL}_r(\mathscr{A}/\mathfrak{a}) \quad &= \quad |\mathfrak{a}|^{r^2} \prod_{\substack{\mathfrak{l}\mid\mathfrak{a} \\ \mathfrak{l}\ prime}} \left(1-\frac{1}{|\mathfrak{l}|}\right)\left(1-\frac{1}{|\mathfrak{l}|^2}\right)\ldots\left(1-\frac{1}{|\mathfrak{l}|^r}\right) \\ &\gg_{\mathscr{K}} \quad \frac{|\mathfrak{a}|^{r^2}}{\log\log|\mathfrak{a}|} \end{aligned}$$

Proof. The lemma is obtained from [Br, Lemma 2.2, p. 1243] and [Br, Lemma 2.3, p. 1244]). □

For the main results of this paper we require more precise information about the degree $[\mathscr{L}\,(\psi\,[\mathfrak{l}^n]) : \mathscr{L}]$, which we deduce from the important results of R. Pink and E. Rütsche [PiRu]. More precisely, we first recall:

Theorem 19. [PiRu, Theorem 0.1, p. 883]
We keep the setting introduced at the beginning of Section 3.6 and assume that

$$\mathrm{End}_{\overline{\mathscr{L}}}(\psi) = \mathscr{A}.$$

Then the image of the representation ρ_ψ is open in $\mathrm{GL}_r\left(\hat{\mathscr{A}}\right)$, that is,

$$|\,\mathrm{GL}_r\left(\hat{\mathscr{A}}\right) : \mathrm{Im}\,\rho_\psi| < \infty.$$

In particular, there exists an integer $i_1(\psi, \mathscr{L}) \in \mathbb{N}$ such that, for any non-zero $a \in \mathscr{A}$,

$$|\mathrm{GL}_r(\mathscr{A}/a\mathscr{A}) : \mathrm{Gal}(\mathscr{L}(\psi[a])/\mathscr{L})| \leq i_1(\psi, \mathscr{L}),$$

and there exists an ideal $I_1(\psi, \mathscr{L})$ of $\mathscr{A}$ such that for any non-zero $a \in \mathscr{A}$ with $(a\mathscr{A}, I_1(\psi, \mathscr{L})) = 1$,

$$\mathrm{Gal}(\mathscr{L}(\psi[a])/\mathscr{L}) \simeq \mathrm{GL}_r(\mathscr{A}/a\mathscr{A}).$$

Note that ψ may not have a non-trivial endomorphism ring. If all endomorphisms of ψ are actually defined over $\mathscr{L}$, then the image of $\rho_{\mathfrak{l},\psi}$ lies in the centralizer $\mathrm{Centr}_{\mathrm{GL}_r(\mathscr{A}_\mathfrak{l})}\left(\mathrm{End}_{\overline{\mathscr{L}}}(\psi)\right)$. In this case, we focus on the representations

$$\rho_{\mathfrak{l},\psi} : G_{\mathscr{L}} \longrightarrow \mathrm{Centr}_{\mathrm{GL}_r(\mathscr{A}_\mathfrak{l})}\left(\mathrm{End}_{\overline{\mathscr{L}}}(\psi)\right),$$

$$\rho_\psi : G_{\mathscr{L}} \longrightarrow \prod_{\mathfrak{l}\neq\infty} \mathrm{Centr}_{\mathrm{GL}_r(\mathscr{A}_\mathfrak{l})}\left(\mathrm{End}_{\overline{\mathscr{L}}}(\psi)\right),$$

and recall:

Theorem 20. [PiRu, Theorem 0.2, p. 883]
We keep the setting introduced at the beginning of Section 3.6 and assume that

$$\mathrm{End}_{\overline{\mathscr{L}}}(\psi) = \mathrm{End}_{\mathscr{L}}(\psi).$$

Then the image of the representation ρ_ψ is open in $\prod_{\mathfrak{l}\neq\infty} \mathrm{Centr}_{\mathrm{GL}_r(\mathscr{A}_\mathfrak{l})}\left(\mathrm{End}_{\overline{\mathscr{L}}}(\psi)\right)$, that is,

$$\left|\prod_{\mathfrak{l}\neq\infty} \mathrm{Centr}_{\mathrm{GL}_r(\mathscr{A}_\mathfrak{l})}\left(\mathrm{End}_{\overline{\mathscr{L}}}(\psi)\right) : \mathrm{Im}\,\rho_\psi\right| < \infty.$$

In particular, there exists an integer $i_2(\psi, \mathscr{L}) \in \mathbb{N}$ such that, for any non-zero $a \in \mathscr{A}$,

$$\left|\mathrm{Centr}_{\mathrm{GL}_r(\mathscr{A}/a\mathscr{A})}\left(\mathrm{End}_{\overline{\mathscr{L}}}(\psi)\right) : \mathrm{Gal}(\mathscr{L}(\psi[a])/\mathscr{L})\right| \leq i_2(\psi, \mathscr{L}),$$

and there exists an ideal $I_2(\psi, \mathscr{L})$ of $\mathscr{A}$ such that for any non-zero $a \in \mathscr{A}$ with $(a\mathscr{A}, I_2(\psi, \mathscr{L})) = 1$,

$$\mathrm{Gal}(\mathscr{L}(\psi[a])/\mathscr{L}) \simeq \mathrm{Centr}_{\mathrm{GL}_r(\mathscr{A}/a\mathscr{A})}\left(\mathrm{End}_{\overline{\mathscr{L}}}(\psi)\right).$$

We will apply these results to deduce a lower bound for the degree $[K(\psi[a]) : K]$ of the a-division field of a generic Drinfeld module $\psi \in \mathrm{Drin}_A(K)$ of rank $r \geq 2$, where K is a finite extension of k. Before we state and prove this bound, let us recall the Drinfeld module analogue of the Tate Conjecture, proven independently in [Tag1]-[Tag2] and [Tam]:

Theorem 21. *(The Tate Conjecture for Drinfeld modules)*
We keep the previous general setting $\mathscr{K}$, $\mathscr{A}$, $\mathscr{L}$. Let ψ_1, $\psi_2 \in \mathrm{Drin}_{\mathscr{A}}(\mathscr{L})$. Then, for any prime $\mathfrak{l}$ of $\mathscr{A}$, the natural map

$$\mathrm{Hom}_{\mathscr{L}}(\psi_1, \psi_2) \otimes_{\mathscr{A}} (\mathscr{A}_{\mathfrak{l}}) \longrightarrow \mathrm{Hom}_{\mathscr{A}_{\mathfrak{l}}[G_{\mathscr{L}}]} (T_{\mathfrak{l}}(\psi_1), T_{\mathfrak{l}}(\psi_2))$$

is an isomorphism.

We are now ready to prove:

Theorem 22. *Let K be a finite extension of k and let $\psi \in \mathrm{Drin}_A(K)$ be of rank $r \geq 2$ and of generic characteristic. Let $\gamma := rank_A\ \mathrm{End}_{\overline{K}}(\psi)$. Then, for any $a \in A \backslash \mathbb{F}_q$, we have*

$$\frac{|a|_\infty^{\frac{r^2}{\gamma}}}{\log\gamma + \log\deg a + \log\log q} \ll_{\psi,K} [K(\psi[a]) : K] \leq |a|_\infty^{\frac{r^2}{\gamma}}$$

Proof. We will follow a strategy used in [Pi], as follows. Let $\tilde{A} := \mathrm{End}_{\overline{K}}(\psi)$ and let F be the field of fractions of $\tilde{A}$. By Theorem 10, all endomorphisms $f \in \tilde{A}$ are defined over a finite extension $\tilde{K}$ of K. Thus, after identifying A with its image $\psi(A) \subseteq \tilde{A}$, we can extend $\psi : A \longrightarrow K\{\tau\}$ tautologically to a homomorphism

$$\tilde{\psi} : \tilde{A} \longrightarrow \tilde{K}\{\tau\}.$$

This is again a Drinfeld module, with the difference that $\tilde{A}$ may not be a *maximal* order in $\tilde{K}$. To fix this, we modify $\tilde{\psi}$ by a suitable isogeny, using results of D. Hayes [Ha].

Indeed, we let $\mathscr{A}$ be the normalization of $\tilde{A}$ in $\tilde{K}$. Then, by [Ha, Proposition 3.2, p. 182], there exists a Drinfeld module

$$\overline{\psi} : \mathscr{A} \longrightarrow \overline{K}\{\tau\}$$

such that $\overline{\psi}|_{\tilde{A}}$ is K-isogenous to $\tilde{\psi}$. Moreover, $\overline{\psi}$ may be chosen such that the restriction $\overline{\psi}|_{\tilde{A}}$ is defined over K.

Now let $\mathscr{K}$ be the finite field extension of K generated by the coefficients of all endomorphisms in $\mathrm{End}_{\overline{K}}(\overline{\psi})$. By Theorem 21, all the endomorphisms of $\overline{\psi}$ over $\overline{K}$ are defined already over K^{sep}. Thus $\mathscr{K}$ is a separable Galois extension of K. Moreover, by construction, the Galois group $\mathrm{Gal}(\mathscr{K}/K)$ acts on F, and, again by Theorem 21, it acts faithfully.

Let

$$\Psi : \mathscr{A} \longrightarrow \mathscr{K}\{\tau\}$$

be the tautological extension of $\overline{\psi}$. This is a generic Drinfeld module of rank

$$R := \frac{r}{\gamma}$$

satisfying $\mathrm{End}_{\overline{\mathscr{K}}}(\Psi) = \mathrm{End}_{\mathscr{K}}(\Psi) = \mathscr{A}$. By Theorem 20, the image of the representation

$$\rho_\Psi : G_{\mathscr{K}} \longrightarrow \prod_{\mathfrak{l} \neq \infty} \mathrm{Centr}_{\mathrm{GL}_R(\mathscr{A}_{\mathfrak{l}})}(\mathscr{A}) \simeq \prod_{\mathfrak{l} \neq \infty} \mathrm{GL}_R(\mathscr{A}_{\mathfrak{l}})$$

is open. In particular, there exists an ideal $I(\Psi,\mathscr{K})$ of $\mathscr{A}$ such that, for any $a\in A$ with $a\mathscr{A}$ coprime to $I(\Psi,\mathscr{K})$, we have

$$\mathrm{Gal}(\mathscr{K}(\Psi[a])/\mathscr{K})\simeq \mathrm{GL}_R(\mathscr{A}/a\mathscr{A}). \tag{12}$$

Since $\mathscr{A}$ is a Dedekind domain, by Lemma 18 we deduce that, for any a as above,

$$\frac{|a\mathscr{A}|^{R^2}}{\log\log|a\mathscr{A}|}\ll_{\mathscr{K}} \#\,\mathrm{GL}_R(\mathscr{A}/a\mathscr{A})\leq |a\mathscr{A}|^{R^2}, \tag{13}$$

where $|a\mathscr{A}|:=\#(\mathscr{A}/a\mathscr{A})$.

Remark that $\#(\mathscr{A}/a\mathscr{A})=\#(A/aA)^\gamma=|a|_\infty^\gamma$. Therefore (12) and (13) imply that, for any $a\in A$ with $a\mathscr{A}$ coprime to $I(\Psi,\mathscr{K})$, we have

$$\frac{|a|_\infty^{\frac{r^2}{\gamma}}}{\log\gamma+\log\deg a+\log\log q}\ll_{\mathscr{K}}[\mathscr{K}(\Psi[a]):\mathscr{K}]\leq |a|_\infty^{\frac{r^2}{\gamma}}.$$

Finally, recalling the construction and properties of $\tilde{\psi},\overline{\psi}$ and Ψ in relation to ψ, we deduce the upper and lower bounds stated in the theorem. □

3.7. **Arithmetic in division fields.** Let K be a finite field extension of k and let $\psi\in\mathrm{Drin}_A(K)$ of generic characteristic and rank $r\geq 1$. For $a\in A\backslash\mathbb{F}_q$, we consider the division field $K(\psi[a])$ and focus on providing useful characterizations and properties of the primes splitting completely in the extension $K(\psi[a])/K$. We start with:

Proposition 23. *(Characterization of primes splitting completely in division fields)*
Let K be a finite field extension of k and let $\psi\in\mathrm{Drin}_A(K)$ be of generic characteristic and rank $r\geq 1$. Let $\wp\in\mathcal{P}_\psi$ and let $m\in A^{(1)}$ be such that $\gcd(m,p)=1$, where $\wp\cap A=pA$. Then $\psi(\mathbb{F}_\wp)$ contains an isomorphic copy of $(A/mA)^r$ if and only if $\wp$ splits completely in $K(\psi[m])/K$. Consequently, given $d\in A^{(1)}$ with $\gcd(d,p)=1$, we have that $d_{1,\wp}(\psi)=d$ if and only if $\wp$ splits completely in $K(\psi[d])/K$ and $\wp$ does not split completely in $K(\psi[d\ell])/K$ for any prime $\ell\in A$ such that $\ell\neq p$.

Proof. Let $\pi_\wp$ be the Frobenius automorphism of $\mathbb{F}_\wp$. Note that $\mathrm{Ker}(\pi_\wp-1)=\psi(\mathbb{F}_\wp)$. Since $\gcd(m,p)=1$, Theorem 11 tells us that $(\psi\otimes\mathbb{F}_\wp)[m]\simeq_A (A/mA)^r$. Therefore, $\psi(\mathbb{F}_\wp)$ contains an isomorphic copy of $(A/mA)^r$ if and only if $(\psi\otimes\mathbb{F}_\wp)[m]\leq_A\psi(\mathbb{F}_\wp)=\mathrm{Ker}(\pi_\wp-1)$.

If $\sigma_\wp$ denotes the Frobenius at $\wp$ in $K(\psi[m])/K$, then $(\psi\otimes\mathbb{F}_\wp)[m]\leq_A\mathrm{Ker}(\pi_\wp-1)$ if and only if $\psi[m]\leq_A\mathrm{Ker}\,(\sigma_\wp-1)$. This last statement is equivalent to $\sigma_\wp$ acting trivially on $\psi[m]$, and hence to $\wp$ splitting completely in $K(\psi[m])/K$.

□

Now let $\wp \in \mathcal{P}_\psi$ and let $\mathfrak{l} = \ell A$ be a prime of k such that $\mathfrak{l} \neq \wp \cap A$. The **characteristic poynomial of the Frobenius $\sigma_\wp$ at $\wp$**, defined by

$$\begin{aligned} P^{\mathfrak{l}}_{\psi,\wp}(X) &:= \det(X\ \mathrm{Id} - \rho_{\psi,\mathfrak{l}}(\sigma_\wp)) \\ &= X^r + a_{r-1,\wp}(\psi)X^{r-1} + \ldots + a_{1,\wp}(\psi)X + a_{0,\wp}(\psi) \in A_{\mathfrak{l}}[X], \end{aligned}$$

is very useful in describing further properties of $\wp$ when it splits completely in a division field of K. We recall the basic properties of this polynomial:

Theorem 24. [Ge, Corollary 3.4, p. 193; Theorem 5.1, p. 199]
Let K be a finite field extension of k and let $\psi \in \mathrm{Drin}_A(K)$ be of generic characteristic and rank $r \geq 1$. Let $\wp \in \mathcal{P}_\psi$ and let $\mathfrak{l} = \ell A$ be a prime of k such that $\mathfrak{l} \neq \wp \cap A$. Then:

(i) *$P^{\mathfrak{l}}_{\psi,\wp}(X) \in A[x]$; in particular, $P^{\mathfrak{l}}_{\psi,\wp}(X)$ is independent of $\mathfrak{l}$, and, as such, we may drop the superscript $\mathfrak{l}$ from notation and simply write $P_{\psi,\wp}(X)$.*

(ii) *There exists $u_\wp(\psi) \in \mathbb{F}_q^*$ such that $a_{0,\wp}(\psi) = u_\wp(\psi)p^{m_\wp}$, where, we recall, $m_\wp := [\mathbb{F}_\wp : \mathbb{F}_{\mathfrak{p}}]$.*

(iii) *The roots of $P_{\psi,\wp}(X)$ have $|\cdot|_\infty$-norm less than or equal to $|\wp|_\infty^{\frac{1}{r}}$.*

(iv) *$|a_{i,\wp}(\psi)|_\infty \leq |\wp|_\infty^{\frac{r-i}{r}}$ for all $0 \leq i \leq r-1$.*

(v) *$P_{\psi,\wp}(1)A = \chi(\psi(\mathbb{F}_\wp))$, where, we recall, $\chi(\psi(\mathbb{F}_\wp))$ denotes the Euler-Poincaré characteristic of $\psi(\mathbb{F}_\wp)$.*

The characteristic polynomial $P_{\psi,\wp}$ is relevant to the characterization of the primes splitting completely in a division field of ψ, as follows.

Proposition 25. *Let K be a finite field extension of k and let $\psi \in \mathrm{Drin}_A(K)$ be of generic characteristic and rank $r \geq 1$. Let $\wp \in \mathcal{P}_\psi$ and let $a \in A \backslash \mathbb{F}_q$ be such that $\gcd(a,p) = 1$, where $\wp \cap A = pA$. If $\wp$ splits completely in $K(\psi[a])$, then $a^r | P_{\psi,\wp}(1)$.*

Proof. Let $\pi_\wp$ be the $|\wp|_\infty$-power Frobenius on $\mathbb{F}_\wp$. Since $\wp$ splits completely in $K(\psi[a])$, $\sigma_\wp$ acts trivially on $\psi[a]$, and so $(\psi \otimes \mathbb{F}_\wp)[d] \leq_A \mathrm{Ker}(\pi_\wp - 1)$. Recalling the structure of the torsion of $\psi \otimes \mathbb{F}_\wp$, we deduce that $\psi(\mathbb{F}_\wp)$ contains an isomorphic copy of $(A/dA)^r$. By taking the Euler-Poincaré characteristic and by invoking part (v) of Proposition 24, we then deduce the desired divisibility relation. □

By combining Proposition 25 with the results of [He] providing a Drinfeld module analoque of the Weil pairing for elliptic curves, we obtain:

Theorem 26. *(Properties of primes splitting completely in division fields)*
Let K be a finite field extension of k and let $\psi \in \mathrm{Drin}_A(K)$ be of generic characteristic and rank $r \geq 2$. Then there exists $\psi^1 \in \mathrm{Drin}_A(K)$, of generic characteristic and of rank 1, uniquely determined up to $\overline{K}$-isomorphism, such that:

(i) *$\mathcal{P}_\psi \subseteq \mathcal{P}_{\psi^1}$;*

(ii) *for any* $\wp \in \mathcal{P}_\psi$*, the characteristic polynomials of* ψ *and* ψ^1 *at* $\wp$ *satisfy the relation:*

$$P_{\psi,\wp}(X) = X^r + a_{r-1,\wp}(\psi)X^{r-1} + \ldots + a_1(\psi,\wp)X + u_\wp(\psi)p^{m_\wp},$$

$$P_{\psi^1,\wp}(X) = X + (-1)^{r-1}u_\wp(\psi)p^{m_\wp},$$

for some $u_\wp(\psi) \in \mathbb{F}_q^*$*;*

(iii) *for any* $\wp \in \mathcal{P}_\psi$ *and any* $a \in A\backslash\mathbb{F}_q$ *coprime to* p*, where* $\wp \cap A = pA$*, we have that, if* $\wp$ *splits completely in* $K(\psi[a])$*, then:*

(iii1) $\wp$ *also splits completely in* $K(\psi^1[a])$*;*

(iii2) $a^r | P_{\psi,\wp}(1)$*;*

(iii3) $a | P_{\psi^1,\wp}(1)$*.*

Proof. See [CoSh, Proposition 10]. □

4. The Chebotarev density theorem

Let K be a finite field extension of k and let K'/K be a finite Galois extension. In this section, we recall an effective version of the Chebotarev Density Theorem for K'/K, as proven in [MuSc].

Let $g_{K'}$ and g_K be the genera of K' and K, respectively, and let $c_{K'}$ denote the degree of the constant field $\mathbb{F}_{K'}$ of K' over $\mathbb{F}_K$, that is,

$$c_{K'} := [K' \cap \overline{\mathbb{F}}_K : \mathbb{F}_K].$$

Let

$$D := \sum_{\wp \text{ ramified in } K'/K} \deg_K \wp.$$

Let $x \in \mathbb{N}$ and set

$$\Pi(x; K'/K) := \#\{\wp \text{ unramified in } K'/K : \deg_K \wp = x\}.$$

For $C \subseteq \mathrm{Gal}(K'/K)$ a conjugacy class, set

$$\Pi_C(x; K'/K) := \#\{\wp \text{ unramified in } K'/K : \deg_K \wp = x, \sigma_\wp = C\},$$

where $\sigma_\wp$ is the Frobenius at $\wp$ in K'/K. Note that, in particular, $\Pi_1(x; K'/K)$ denotes the number of degree x primes of K which split completely in K'. Let $a_C \in \mathbb{N}$ be defined by the property that the restriction of C to $\mathbb{F}_{K'}$ is τ^{a_C}.

Theorem 27. [MuSc, Theorem 1, p. 524]
We keep the above setting and notation.

(i) *If* $x \not\equiv a_C \pmod{c_{K'}}$*, then* $\Pi_C(x; K'/K) = 0$*.*

(ii) *If* $x \equiv a_C \pmod{c_{K'}}$*, then*

$$\left|\Pi_C(x; K'/K) - c_{K'}\frac{|C|}{|G|}\Pi(x; K'/K)\right| \leq 2g_{K'}\frac{|C|}{|G|}\frac{q^{\frac{c_K x}{2}}}{x} + 2(2g_K+1)|C|\frac{q^{\frac{c_K x}{2}}}{x} + \left(1 + \frac{|C|}{x}\right)D.$$

Our main application of Theorem 27 is when K' is a division field of a generic Drinfeld module $\psi \in \mathrm{Drin}_A(K)$ and when $C = \{1\}$. For ease of understanding, we record a restatement of this theorem in our desired setting:

Theorem 28. *Let K be a finite field extension of k and let $\psi \in \mathrm{Drin}_A(K)$ be of generic characteristic. Let $a \in A\backslash\mathbb{F}_q$. Let $x \in \mathbb{N}$ and define*

$$c_a(x) := \begin{cases} c_a & \text{if } c_a | x, \\ 0 & \text{else}, \end{cases} \tag{14}$$

where c_a denotes the degree of the constant field extension of $K(\psi[a])$ over $\mathbb{F}_K$ (see (10)). Then

$$\Pi_1(x; K(\psi[a])/K) = \frac{c_a(x)}{[K(\psi[a]) : K]} \cdot \frac{q^{c_K x}}{x} + \mathrm{O}_{\psi,K}\left(\frac{q^{\frac{c_K x}{2}}}{x} \deg a\right).$$

Proof. Using the effective Prime Number Theorem for K (see (6)) and Theorem 27 with $K' = K(\psi[a])$, $C = \{1\}$, and hence with $a_C = 0$, we obtain

$$\Pi_1(x; K(\psi[a])/K) = \frac{c_a(x)}{[K(\psi[a]) : K]} \cdot \frac{q^{c_K x}}{x} + \mathrm{O}\left(\left(2g_a \cdot \frac{1}{[K(\psi[a]) : K]} + 2(2g_K + 1)\right) \cdot \frac{q^{\frac{c_K x}{2}}}{x} + \left(1 + \frac{1}{x}\right) D\right),$$

where

$$D := \sum_{\substack{\wp \in \mathcal{P}_\psi \\ \wp \text{ ramified in } K(\psi[a])/K}} \deg_K \wp.$$

By Theorem 14, $D \ll_K \deg a$. Combining this with Proposition 17, we obtain

$$\begin{aligned} \left(2g_a \cdot \frac{1}{[K(\psi[a]) : K]} + 2(2g_K + 1)\right) \cdot \frac{q^{\frac{c_K x}{2}}}{x} + \left(1 + \frac{1}{x}\right) D &\ll_K \frac{G(\psi, K) \cdot [K(\psi[a]) : K] \cdot \deg a}{[K(\psi[a]) : K]} \cdot \frac{q^{\frac{c_K x}{2}}}{x} \\ &\quad + \frac{x+1}{x} \cdot \deg a \\ &\ll_K G(\psi, K) \cdot \frac{q^{\frac{c_K x}{2}}}{x} \cdot \deg a. \end{aligned}$$

□

5. Proof of Theorems 1 and 2

Let K/k be a finite field extension and let $\psi : A \longrightarrow K\{\tau\}$ be a generic Drinfeld A-module over K, of rank $r \geq 2$. Let $d \in A^{(1)}$. For a fixed $x \in \mathbb{N}$, let

$$\mathscr{D}(\psi, x) := \#\{\wp \in \mathcal{P}_\psi : \deg_K \wp = x,\ d_{1,\wp}(\psi) = d\}.$$

Our first goal is to derive an asymptotic formula for this function, as $x \to \infty$.

We start by noting that, for any prime $\wp \in \mathcal{P}_\psi$ such that $\gcd(d, p) = 1$ (where, as usual, $\wp \cap A = pA$), we have $d = d_{1,\wp}(\psi)$ if and only if $\psi(\mathbb{F}_\wp) \geq_A (A/dA)^r$ and $\psi(\mathbb{F}_\wp) \not\geq_A (A/\ell dA)^r$ for all primes $\ell \in A^{(1)}$. Hence, by the inclusion-exclusion principle and by Proposition 23,

$$\mathscr{D}(\psi, x) = \sum_{\substack{m \in A^{(1)} \\ \deg m \leq \frac{c_K x}{r}}} \mu_A(m) \Pi_1(x; K(\psi[md])/K), \tag{15}$$

where, for square-free m, the field extension $K(\psi[md])/K$ is obtained via field composition

$$\prod_{\substack{\ell \mid m \\ \ell \text{ prime}}} K(\psi[\ell d]) = K(\psi[\operatorname{lcm}\{\ell d : \ell \mid m\}]) = K(\psi[md]),$$

and where, we recall,

$$\Pi_1(x; K(\psi[md])/K) := \#\{\wp \in \mathcal{P}_\psi : \deg_K \wp = x, \wp \text{ splits completely in } K(\psi[md])/K\}.$$

The range of $\deg m$ in the summation on the right-hand side of (15) is derived from the restriction

$$(A/mdA)^r \leq_A \psi(\mathbb{F}_\wp),$$

hence from the divisibility relation

$$m^r d^r \mid \chi(\psi(\mathbb{F}_\wp))$$

obtained by taking Euler-Poincaré characteristic on both sides. Indeed, since $|\chi(\psi(\mathbb{F}_\wp))|_\infty = |\wp|_\infty = q^{c_K x}$, the above gives

$$\deg m \leq \frac{c_K x}{r}.$$

The obvious tool in estimating $\mathscr{D}(\psi, x)$ is the effective Chebotarev Density Theorem (Theorem 28). However, for $r = 2$, this is insufficient. As such, we split the sum into two parts, apply Theorem 28 to the first, and find a different approach for the second. To be precise, we write

$$\mathscr{D}(\psi, x) = \mathscr{D}_1(\psi, x, y) + \mathscr{D}_2(\psi, x, y) \tag{16}$$

for some positive real number $y = y(x)$, to be chosen optimally later, where

$$\mathscr{D}_1(\psi, x, y) := \sum_{\substack{m \in A^{(1)} \\ \deg m \leq y}} \mu_A(m) \Pi_1(x; K(\psi[md])/K)$$

and

$$\mathscr{D}_2(\psi, x, y) := \sum_{\substack{m \in A^{(1)} \\ y < \deg m \leq \frac{c_K x}{r}}} \mu_A(m) \Pi_1(x; K(\psi[md])/K).$$

By applying Theorem 28 and Lemma 4, we obtain

$$\mathscr{D}_1(\psi, x, y) = \frac{q^{c_K x}}{x} \sum_{\substack{m \in A^{(1)} \\ \deg m \leq y}} \frac{\mu_A(m) c_{md}(x)}{[K(\psi[md]) : K]} + \mathrm{O}_{\psi, K, d}\left(\frac{q^{\frac{c_K x}{2} + y} y}{x}\right). \tag{17}$$

Now let

$$\gamma := \operatorname{rank}_A \operatorname{End}_{\overline{K}}(\psi).$$

By Proposition 16, Theorem 22, and Lemma 5, we obtain

$$\sum_{\substack{m \in A^{(1)} \\ \deg m > y}} \frac{\mu_A(m) c_{md}(x)}{[K(\psi[md]) : K]} \ll_{\psi, K} \sum_{\substack{m \in A^{(1)} \\ \deg m > y}} \frac{\log \deg(md) + \log\log q}{q^{\frac{r^2 \deg(md)}{\gamma}}} \ll \frac{\log y}{q^{\left(\frac{r^2}{\gamma} - 1\right) y} \log q}. \tag{18}$$

Thus

$$\mathscr{D}_1(\psi,x,y)=\frac{q^{c_K x}}{x}\sum_{m\in A^{(1)}}\frac{\mu_A(m)c_{md}(x)}{[K(\psi[md]):K]}+\mathrm{O}_{\psi,K,d}\left(\frac{q^{\frac{c_K x}{2}+y}y}{x}\right)+\mathrm{O}_{\psi,K}\left(\frac{q^{c_K x-\left(\frac{r^2}{\gamma}-1\right)y}\log y}{\log q}\right). \quad (19)$$

To estimate $\mathscr{D}_2(\psi,x,y)$ from above, we make use of van der Heiden's construction of the analogue of the Weil pairing for ψ, as well as of the average over m. More precisely, we appeal to Theorem 26 and rely on the properties of the rank 1 Drinfeld A-module $\psi^1\in\mathrm{Drin}_A(K)$ associated to ψ, as follows.

By part (iii1) of Theorem 26, if $\wp$ splits completely in $K(\psi[md])/K$, then $\wp$ splits completely in $K(\psi^1[md])/K$. Using the characteristic polynomials at $\wp$ associated to ψ and ψ^1, by part (ii) of Theorem 26, this implies that

$$m^r d^r | 1+a_\wp(\psi)+u_\wp(\psi)p^{m_\wp}$$

and

$$md|1+(-1)^{r-1}u_\wp(\psi)p^{m_\wp},$$

where, we recall,

$$P_{\wp,\psi}(X)=X^r+a_{r-1,\wp}(\psi)X^{r-1}+\ldots+a_{1,\wp}(\psi)X+u_\wp(\psi)p^{m_\wp}\in A[X]$$

with $u_\wp(\psi)\in\mathbb{F}_q^*$, and where we define

$$a_\wp(\psi):=a_{r-1,\wp}(\psi)+\ldots+a_{1,\wp}(\psi).$$

By part (iv) of Theorem 24, we obtain that

$$\deg a_\wp(\psi)\le\frac{(r-1)c_K\deg_K\wp}{r}.$$

Therefore

$$\mathscr{D}_2(\psi,x,y)\quad\le\quad\sum_{\substack{m\in A^{(1)}\\ y<\deg m\le\frac{c_K x}{r}}}\sum_{u\in\mathbb{F}_q^*}\sum_{\substack{a\in A\\ \deg a\le\frac{(r-1)c_K x}{r}}}\sum_{\substack{\wp\in\mathcal{P}_\psi\\ \deg_K\wp=x\\ a_\wp(\psi)=a,u_\wp(\psi)=u\\ m^r d^r|1+a_\wp(\psi)+u_\wp(\psi)p^{m_\wp}\\ md|1+(-1)^{r-1}u_\wp(\psi)p^{m_\wp}}}1.$$

To simplify notation, let us define, for each $a\in A$,

$$\tilde{a}:=\begin{cases}2+a & \text{for } r \text{ even},\\ a & \text{for } r \text{ odd}.\end{cases} \quad (20)$$

Thus

$$\mathscr{D}_2(\psi,x,y)\le\sum_{\substack{m\in A^{(1)}\\ y<\deg m\le\frac{c_K x}{r}}}\sum_{u\in\mathbb{F}_q^*}\sum_{\substack{a\in A\\ \deg a\le\frac{(r-1)c_K x}{r}\\ md|\tilde{a}}}\sum_{\substack{\wp\in\mathcal{P}_\psi\\ \deg_K\wp=x\\ m^r d^r|1+a+up^{m_\wp}}}1.$$

We now consider the innermost sum above. Using diagram (9), we see that

$$\deg p^{m_\wp}=m_\wp\deg p=c_K\deg_K\wp=c_K x.$$

We also see that, by part (i) of Lemma 4, for fixed $a \in A$ and $u \in \mathbb{F}_q^*$, there exist at most $q^{c_K x - r\deg m + 1}$ primes $p \in A$ of degree $\frac{c_K x}{m_\wp}$ such that $m^r | 1 + a + up^{m_\wp}$. But there are at most $[K : k]$ primes in K lying above a fixed prime $p \in A$. Therefore

$$\sum_{\substack{\wp \in \mathcal{P}_\psi \\ \deg_K \wp = x \\ m^r | 1 + a + up^{m_\wp}}} 1 \ll_K q^{c_K x - r\deg m + 1} \ll q^{c_K x - r \deg m}.$$

Continuing, we deduce that

$$\begin{aligned}
\mathscr{D}_2(\psi, x, y) &\ll_{K,d} \sum_{\substack{m \in A^{(1)} \\ y < \deg m \le \frac{c_K x}{r}}} \sum_{u \in \mathbb{F}_q^*} \sum_{\substack{a \in A \\ \deg a \le \frac{(r-1)c_K x}{r} \\ m | \tilde{a}}} q^{c_K x - r \deg m} \\
&= q^{c_K x} \sum_{\substack{m \in A^{(1)} \\ y < \deg m \le \frac{c_K x}{r}}} q^{-r\deg m} \sum_{u \in \mathbb{F}_q^*} \sum_{\substack{a \in A \\ \deg a \le \frac{(r-1)c_K x}{r} \\ \tilde{a} \neq 0 \\ m | \tilde{a}}} 1 \\
&\quad + q^{c_K x} \sum_{\substack{m \in A^{(1)} \\ y < \deg m \le \frac{c_K x}{r}}} q^{-r\deg m} \sum_{u \in \mathbb{F}_q^*} \sum_{\substack{a \in A \\ \deg a \le \frac{(r-1)c_K x}{r} \\ \tilde{a} = 0}} 1 \\
&=: \mathscr{D}_{2,1}(\psi, x, y) + \mathscr{D}_{2,2}(\psi, x, y).
\end{aligned}$$

To estimate $\mathscr{D}_{2,1}(\psi, x, y)$ from above, we note that

$$\mathscr{D}_{2,1}(\psi, x, y) \le q^{c_K x + 1} \sum_{\substack{m \in A^{(1)} \\ y < \deg m \le \frac{c_K x}{r}}} q^{-r\deg m} \sum_{\substack{\alpha \in A \\ \deg \alpha \le \frac{(r-1)c_K x}{r} - \deg m}} 1,$$

which, by part (i) of Lemma 4 and part (i) of Lemma 5, is

$$\ll q^{c_K x + 1} \sum_{\substack{m \in A^{(1)} \\ y < \deg m \le \frac{c_K x}{r}}} q^{-r\deg m} q^{\frac{(r-1)c_K x}{r} - \deg m} \ll q^{\frac{(2r-1)c_K x}{r} - ry}.$$

To estimate $\mathscr{D}_{2,2}(\psi, x, y)$ from above, we note that its innermost sum has only one term, hence, by part (ii) of Lemma 5,

$$\mathscr{D}_{2,2}(\psi, x, y) \ll q^{c_K x - (r-1)y}.$$

Combining these estimates, we obtain that

$$\mathscr{D}_2(\psi, x, y) \ll_{K,d} q^{\frac{(2r-1)c_K x}{r} - ry} + q^{c_K x - (r-1)y}.$$

Plugging this back into (16) and appealing to (19), we deduce that

$$\begin{aligned}
\mathscr{D}(\psi, x) &= \frac{q^{c_K x}}{x} \sum_{m \in A^{(1)}} \frac{\mu_A(m) c_{md}(x)}{[K(\psi[md]) : K]} \\
&\quad + \mathrm{O}_{\psi,K,d}\left(\frac{q^{\frac{c_K x}{2} + y} y}{x}\right) + \mathrm{O}_{\psi,K}\left(\frac{q^{c_K x - \left(\frac{r^2}{\gamma} - 1\right)y} \log y}{\log q}\right) + \mathrm{O}_{K,d}\left(q^{\frac{(2r-1)c_K x}{r} - ry} + q^{c_K x - (r-1)y}\right).
\end{aligned}$$

Finally, we choose y as follows:

$$y := \begin{cases} \frac{3r-2}{2r(r+1)} c_K x & \text{if } r = 2, 3, \\ \frac{1}{r} c_K x & \text{if } r \geq 4. \end{cases} \tag{21}$$

With this choice, we obtain the effective asymptotic formulae:

$$\mathscr{D}(\psi, x) = \frac{q^{c_K x}}{x} \sum_{m \in A^{(1)}} \frac{\mu_A(m) c_{md}(x)}{[K(\psi[md]) : K]} + \begin{cases} \mathrm{O}_{\psi,K,d}\left(q^{\frac{5c_K x}{6}}\right) & \text{if } r = 2, \\ \mathrm{O}_{\psi,K,d}\left(q^{\frac{19c_K x}{24}}\right) & \text{if } r = 3, \\ \mathrm{O}_{\psi,K,d}\left(q^{\frac{(r+2)c_K x}{2r}}\right) & \text{if } r \geq 4. \end{cases} \tag{22}$$

This completes the first part of Theorem 1.

Remark 29.

(i) *Formula (22) is stronger than the asymptotic formula (7) stated in Theorem 1, as it provides us with explicit error terms. Moreover, these error terms carry significant savings in powers of* $q^{c_K x}$.

(ii) *For* $r \geq 4$, *the splitting of* $\mathscr{D}(\psi, x)$ *into two parts, as in (16), is unnecessary. The proof of Theorem 1 in this case is solely an application of the effective Chebotarev Density Theorem for the division fields of* ψ.

(iii) *For* $r = 3$, *the splitting of* $\mathscr{D}(\psi, x)$ *into two parts, as in (16), is also unnecessary in order to obtain the asymptotic formula (7). In our proof, we do so in this case in order to obtain a saving in the final error term:* $\mathrm{O}_{\psi,K,d}\left(q^{\frac{19c_K x}{24}}\right)$ *using (16) and the approach therein for estimating* $\mathscr{D}_2(\psi, x, y)$, *versus* $\mathrm{O}_{\psi,K,d}\left(q^{\frac{5c_K x}{6}}\right)$ *using only the effective Chebotarev Density Theorem (and the choice* $y := \frac{1}{3} c_K x$*).*

(iv) *The error terms in (22) may be improved with additional techniques. For example, for the case* q *odd,* $r = 2$, $\gamma = 2$, *and* $K = k$, *in* [CoSh] *we proved the formula*

$$\mathscr{D}(\psi, x) = \frac{q^x}{x} \sum_{m \in A^{(1)}} \frac{\mu_A(m) c_{md}(x)}{[k(\psi[md]) : k]} + \mathrm{O}_{\psi,k,d}\left(q^{\frac{3x}{4}}\right).$$

Our second goal is to prove that the Dirichlet density of the set $\{\wp \in \mathcal{P}_\psi : d_{1,\wp}(\psi) = d\}$ exists and equals $\sum_{m \in A^{(1)}} \frac{\mu_A(m)}{[K(\psi[md]) : K]}$. For this, let $s > 1$ and consider the sum

$$\begin{aligned} \sum_{\substack{\wp \in \mathcal{P}_\psi \\ d_{1,\wp}(\psi) = d}} q^{-s c_K \deg_K \wp} &= \sum_{x \geq 1} q^{-s c_K} \mathscr{D}(\psi, x) \\ &= \sum_{m \in A^{(1)}} \frac{\mu_A(m)}{[K(\psi[md]) : K]} \sum_{x \geq 1} \frac{q^{(1-s)c_K x} c_{md}(x)}{x} + \mathrm{O}_{\psi,K}\left(\sum_{x \geq 1} q^{(\theta(r)-s)c_K x}\right), \end{aligned} \tag{23}$$

where we used (22) with

$$\theta(r) := \begin{cases} \frac{5}{6} & \text{if } r = 2, \\ \frac{19}{24} & \text{if } r = 3, \\ \frac{r+2}{2r} & \text{if } r \geq 4. \end{cases} \tag{24}$$

By the definition (14) of $c_{md}(x)$, (23) becomes

$$= \sum_{m\in A^{(1)}} \frac{\mu_A(m)}{[K(\psi[md]):K]} \sum_{j\le 1} \frac{q^{(1-s)c_K c_{md} j}}{j} + \mathrm{O}_{\psi,K}\left(\sum_{x\ge 1} q^{(\theta(r)-s)c_K x}\right).$$

Since $s>1$, this may be written as

$$= -\sum_{m\in A^{(1)}} \frac{\mu_A(m)}{[K(\psi[md]):K]} \log\left(1-q^{(1-s)c_K c_{md}}\right) + \mathrm{O}_{\psi,K}\left(\frac{q^{(\theta(r)-s)c_K}}{1-q^{(\theta(r)-s)c_K}}\right).$$

We now calculate

$$\begin{aligned}
\lim_{s\to 1+} \frac{\sum\limits_{\substack{\wp\in\mathcal{P}_\psi \\ d_{1,\wp}(\psi)=d}} q^{-sc_K \deg\wp}}{-\log\left(1-q^{(1-s)c_K}\right)} &= \lim_{s\to 1+}\left[\left(\sum_{m\in A^{(1)}} \frac{\mu_A(m)}{[K(\psi[md]):K]}\right)\frac{\log\left(1-q^{(1-s)c_K c_{md}}\right)}{\log\left(1-q^{(1-s)c_K}\right)}\right. \\
&\quad \left. + \mathrm{O}_{\psi,K}\left(\frac{q^{(\theta(r)-s)c_K}}{\left(1-q^{(\theta(r)-s)c_K}\right)\log\left(1-q^{(1-s)c_K}\right)}\right)\right] \\
&= \sum_{m\in A^{(1)}} \frac{\mu_A(m)}{[K(\psi[md]):K]},
\end{aligned}$$

after an application of l'Hospital and elementary manipulations. This completes the proof of Theorem 1.

The proof of Theorem 2 proceeds in the same way as that of the first part of Theorem 1, after replacing with 1 the factor $\mu_A(m)$ appearing in (15), and, henceforth, in $\mathscr{D}_1(\psi,x,y)$ and $\mathscr{D}_2(\psi,x,y)$ of (16).

6. Proof of Theorem 3

Let K/k be a finite field extension and let $\psi : A \longrightarrow K\{\tau\}$ be a generic Drinfeld A-module over K, of rank 2. Let $\gamma := \mathrm{rank}_A\ \mathrm{End}_{\overline{K}}(\psi)$.

(i) Let $f:(0,\infty)\longrightarrow(0,\infty)$ be such that $\lim\limits_{x\to\infty} f(x)=\infty$ and $f(x)<\frac{x}{2}\ \forall x$. For a fixed $x\in\mathbb{N}$, let

$$\mathcal{E}(\psi,x) := \#\left\{\wp\in\mathcal{P}_\psi : \deg_K\wp = x, |d_{2,\wp}(\psi)|_\infty > \frac{|\wp|_\infty}{q^{c_K f(x)}}\right\}$$

and

$$e(\psi,x) := \#\left\{\wp\in\mathcal{P}_\psi : \deg_K\wp = x, |d_{2,\wp}(\psi)|_\infty < \frac{|\wp|_\infty}{q^{c_K f(x)}}\right\}.$$

Our goal is to derive an asymptotic formula for $\mathcal{E}(\psi,x)$, as $x\to\infty$. More precisely, our goal is to show that $\mathcal{E}(\psi,x)\sim\pi_K(x)$, which is equivalent to showing that

$$e(\psi,x) = \mathrm{o}\left(\pi_K(x)\right).$$

We start with the partition

$$e(\psi,x) = \sum_{d\in A^{(1)}} \sum_{\substack{\wp\in\mathcal{P}_\psi \\ \deg_K\wp = x \\ d_{1,\wp}(\psi)=d \\ |d_{2,\wp}(\psi)|_\infty < \frac{|\wp|_\infty}{q^{c_K f(x)}}}} 1,$$

and remark that, as in the deduction of (15) in the proof of Theorem 1, the condition $d|d_{1,\wp}(\psi)$ imposes the restriction $\deg d \le \frac{c_K x}{2}$. Moreover, the conditions $d_{1,\wp}(\psi) = d$ and $|d_{2,\wp}(\psi)|_\infty < \frac{|\wp|_\infty}{q^{c_K f(x)}}$, coupled with the remark

$$|\wp|_\infty = |\chi(\psi(\mathbb{F}_\wp))|_\infty = |d_{1,\wp}(\psi)|_\infty |d_{2,\wp}(\psi)|_\infty, \tag{25}$$

impose the restriction $c_K f(x) < \deg d$. Thus

$$e(\psi, x) \le \sum_{\substack{d \in A^{(1)} \\ c_K f(x) < \deg d \le \frac{c_K x}{2}}} \#\{\wp \in \mathcal{P}_\psi : \deg_K \wp = x, d|d_{1,\wp}(\psi)\} = \sum_{\substack{d \in A^{(1)} \\ c_K f(x) < \deg d \le \frac{c_K x}{2}}} \Pi_1(x, K(\psi[d])/K),$$

by also using Proposition 23. Using Theorem 2 for the range $\deg d \le \frac{c_K x}{2}$ and Theorem 28 for the range $\deg d \le c_K f(x)$, the above is

$$= \frac{q^{c_K x}}{x} \sum_{\substack{d \in A^{(1)} \\ c_K f(x) < \deg d \le \frac{c_K x}{2}}} \frac{c_d(x)}{[K(\psi[d]) : K]} + \mathrm{O}_{\psi,K}\left(q^{\frac{5c_K x}{6}}\right) + \mathrm{O}_{\psi,K}\left(\frac{q^{\frac{c_K x}{2} + c_K f(x)} f(x)}{x}\right). \tag{26}$$

Reasoning as for (18) in the proof of Theorem 1, the first term becomes

$$\ll_{\psi,K} q^{c_K\left(x - \left(\frac{4}{\gamma} - 1\right) f(x)\right)} \frac{\log f(x)}{x}.$$

Since $\lim_{x \to \infty} f(x) = \infty$ and $f(x) < \frac{x}{2}$, we deduce that $e(\psi, x) = \mathrm{o}(\pi_K(x))$.

Remark 30. *The same proof can be carried through in the case $r = 3$, leading to a weaker result. For $r \ge 4$, however, one will need a more careful analysis that also takes into consideration the behaviour of the intermediate elementary divisors.*

We now show that, when there is $0 < \theta < 1$ such that $f(x) \le \frac{\theta x}{2}$ for all x, the Dirichlet density of the set $\left\{\wp \in \mathcal{P}_\psi : |d_{2,\wp}|_\infty < \frac{|\wp|_\infty}{q^{c_K f(\deg_K \wp)}}\right\}$ equals 0.

Let $s > 1$ and consider the sum

$$\begin{aligned}
&\sum_{\substack{\wp \in \mathcal{P}_\psi \\ |d_{2,\wp}(\psi)|_\infty < \frac{|\wp|_\infty}{q^{c_K f(\deg_K \wp)}}}} q^{-s c_K \deg_K \wp} = \sum_{x \ge 1} q^{-s c_K x} e(\psi, x) \\
\ll &\sum_{x \ge 1} \frac{q^{(1-s)c_K x}}{x} \sum_{\substack{d \in A^{(1)} \\ c_K f(x) < \deg d \le \frac{c_K x}{2}}} \frac{c_d(x)}{[K(\psi[d]) : K]} + \sum_{x \ge 1} q^{\left(\frac{5}{6} - s\right) c_K x} + \sum_{x \ge 1} \frac{q^{\left(\frac{1}{2} - s\right) c_K x + c_K f(x)} f(x)}{x} \\
=: &\; T_1 + T_2 + T_3,
\end{aligned} \tag{27}$$

where we also used the prior estimate (26).

First we focus on T_1. By the definition of $c_d(x)$, we obtain

$$\begin{aligned} T_1 &:= \sum_{x\geq 1} \frac{q^{(1-s)c_K x}}{x} \sum_{\substack{d\in A^{(1)} \\ c_K f(x)<\deg d\leq \frac{c_K x}{2}}} \frac{c_d(x)}{[K(\psi[d]):K]} \\ &= \sum_{d\in A^{(1)}} \sum_{\substack{j\geq 1 \\ c_K f(c_j d)<\deg d\leq \frac{c_K c_d j}{2}}} \frac{q^{(1-s)c_K c_d j}}{j[K(\psi[d]):K]}. \end{aligned} \tag{28}$$

Let $M>0$. Since $\lim_{x\to\infty} f(x)=\infty$, there exists $n(M)\in\mathbb{N}$ such that $f(n)>M$ for all $n\geq n(M)$. We split the inner sum in (28) according to whether $c_d j\geq n(M)$ and $c_d j<n(M)$, and consider each of the two emerging sums separately.

By the above and Theorem 22, we have

$$\begin{aligned} T_{1,1} &:= \sum_{d\in A^{(1)}} \sum_{\substack{j\geq 1 \\ c_d j\geq n(M) \\ c_K f(c_d j)<\deg d\leq \frac{c_K c_d j}{2}}} \frac{q^{(1-s)c_K c_d j}}{j[K(\psi[d]):K]} \\ &\leq \sum_{d\in A^{(1)}} \sum_{\substack{j\geq 1 \\ c_d j\geq n(M) \\ c_K M<\deg d\leq \frac{c_K c_d j}{2}}} \frac{q^{(1-s)c_K c_d j}}{j[K(\psi[d]):K]} \\ &\ll_{\psi,K} \sum_{\substack{d\in A^{(1)} \\ c_K M<\deg d}} \frac{\log\deg d}{|d|_\infty^{\frac{4}{\gamma}}} \sum_{\substack{j\geq 1 \\ c_d j\geq n(M)}} \frac{q^{(1-s)c_K c_d j}}{j}. \end{aligned}$$

Since $s>1$, the latter becomes

$$= \sum_{\substack{d\in A^{(1)} \\ c_K M<\deg d}} \frac{\log\deg d}{|d|_\infty^{\frac{4}{\gamma}}} \left[-\log\left(1-q^{(1-s)c_K c_d}\right) + \sum_{1\leq j\leq n(M)-1} \frac{q^{(1-s)c_K c_d j}}{j} \right].$$

By Lemma 5, this is

$$\ll \frac{\log(c_K M)}{q^{(\frac{4}{\gamma}-1)c_K M}\log q} \left[\left|\log\left(1-q^{(1-s)c_K c_d}\right)\right| + \sum_{1\leq j\leq n(M)-1} \frac{q^{(1-s)c_K c_d j}}{j} \right],$$

which gives that

$$\lim_{s\to 1+} \frac{T_{1,1}}{-\log\left(1-q^{(1-s)c_K}\right)} \ll \frac{\log(c_K M)}{q^{3c_K M}\log q}. \tag{29}$$

We also have

$$T_{1,2} := \sum_{d\in A^{(1)}} \sum_{\substack{j\geq 1 \\ c_d j\geq n(M) \\ c_K f(c_d j)<\deg d\leq \frac{c_K c_d j}{2}}} \frac{q^{(1-s)c_K c_d j}}{j[K(\psi[d]):K]},$$

a finite sum. Since $\lim_{s\to 1+} \frac{q^{(1-s)c_K \alpha}}{\log\left(1-q^{(1-s)c_K}\right)} = 0$ for any $\alpha\in\mathbb{N}$, we deduce that

$$\lim_{s\to 1+} \frac{T_{1,2}}{-\log\left(1-q^{(1-s)c_K}\right)} = 0. \tag{30}$$

By taking $M \to \infty$ and by using (29) and (30), we obtain that

$$\lim_{s\to 1+} \frac{T_1}{-\log\left(1-q^{(1-s)c_K}\right)} = 0. \tag{31}$$

We now focus on T_2 and note that

$$\lim_{s\to 1+} \frac{T_2}{-\log\left(1-q^{(1-s)c_K}\right)} = -\lim_{s\to 1+} \frac{q^{\left(\frac{5}{6}-s\right)c_K}}{\left(1-q^{\left(\frac{5}{6}-s\right)c_K}\right)\log\left(1-q^{(1-s)c_K}\right)} = 0. \tag{32}$$

It remains to focus on T_3. Recalling that now we are assuming that there exists $0 < \theta < 1$ such that $f(x) \leq \frac{\theta x}{2} \ \ \forall x$, we see that

$$\begin{aligned}
\lim_{s\to 1+} \frac{T_3}{-\log\left(1-q^{(1-s)c_K}\right)} &= -\lim_{s\to 1+} \frac{\displaystyle\sum_{x\geq 1} \frac{q^{\left(\frac{1}{2}-s\right)c_K x + c_K f(x)} f(x)}{x}}{\log\left(1-q^{(1-s)c_K}\right)} \\
&\ll \left| \lim_{s\to 1+} \frac{\displaystyle\sum_{x\geq 1} q^{\left(\frac{1}{2}+\theta-s\right)}}{\log\left(1-q^{(1-s)c_K}\right)} \right| \\
&= \left| \lim_{s\to 1+} \frac{q^{\left(\frac{1}{2}+\theta-s\right)c_K}\left(1-q^{\left(\frac{1}{2}+\theta-s\right)c_K}\right)^{-1}}{\log\left(1-q^{(1-s)c_K}\right)} \right| \\
&= 0.
\end{aligned} \tag{33}$$

By combining (27) with (31) - (33), we obtain

$$\lim_{s\to 1+} \frac{\displaystyle\sum_{\wp\in\mathcal{P}_\psi} \ \sum_{|d_{2,\wp}(\psi)|_\infty < \frac{|\wp|_\infty}{q^{c_K f(\deg_K \wp)}}} q^{-sc_K \deg_K \wp}}{-\log\left(1-q^{(1-s)c_K}\right)} = 0.$$

This completes the proof of the first part of Theorem 3.

(ii) By using (25) and Lemma 7, we obtain

$$\begin{aligned}
\sum_{\substack{\wp\in\mathcal{P}_\psi \\ \deg_K \wp = x}} |d_{2,\wp}(\psi)|_\infty &= q^{c_K x} \sum_{\substack{\wp\in\mathcal{P}_\psi \\ \deg_K \wp = x}} \frac{1}{|d_{1,\wp}(\psi)|_\infty} \\
&= q^{c_K x} \sum_{\substack{d\in A^{(1)} \\ \deg d \leq \frac{c_K x}{2}}} \ \sum_{\substack{m,n\in A^{(1)} \\ mn=d}} \frac{\mu_A(m)}{|n|_\infty} \Pi_1(x, K(\psi[d])/K),
\end{aligned}$$

where, in the last line above, we also applied Proposition 23.

We proceed as in the proof of Theorem 1 and split the sum over d into two parts, according to whether $\deg d \leq \frac{c_K x}{3}$ and $\frac{c_K x}{3} < \deg d \leq \frac{c_K x}{2}$ (recall the choice of the parameter y made in (21)). More precisely, by using Lemma 8 and the upper bound $\frac{\Phi_A(d)}{|d|_\infty} \leq 1$, as well as the same reasoning as for estimating $\mathscr{D}_1(\psi, x, y)$

and $\mathscr{D}_2(\psi,x,y)$, we obtain

$$\sum_{\substack{d\in A^{(1)}\\ \deg d\le \frac{c_K x}{3}}}\sum_{mn=d}\frac{\mu_A(m)}{|n|_\infty}\Pi_1(x,K(\psi[d])/K)=\frac{q^{c_K x}}{x}\sum_{d\in A^{(1)}}\frac{c_d(x)}{[K(\psi[d]):K]}\sum_{\substack{m,n\in A^{(1)}\\ mn=d}}\frac{\mu_A(m)}{|n|_\infty}+\mathrm{O}_{\psi,K}\left(q^{\frac{5c_K x}{6}}\right)$$

and

$$\sum_{\substack{d\in A^{(1)}\\ \frac{c_K x}{3}<\deg d\le\frac{c_K x}{2}}}\sum_{\substack{m,n\in A^{(1)}\\ mn=d}}\frac{\mu_A(m)}{|n|_\infty}\Pi_1(x,K(\psi[d])/K)\ll q^{\frac{5c_K x}{6}}.$$

This proves the asymptotic formula

$$\frac{1}{q^{c_K x}}\sum_{\substack{\wp\in\mathcal{P}_\psi\\ \deg_K\wp=x}}|d_{2,\wp}(\psi)|_\infty=\frac{q^{c_K x}}{x}\sum_{d\in A^{(1)}}\frac{c_d(x)}{[K(\psi[d]):K]}\sum_{\substack{m,n\in A^{(1)}\\ mn=d}}\frac{\mu_A(m)}{|n|_\infty}+\mathrm{O}_{\psi,K}\left(q^{\frac{5c_K x}{6}}\right),\tag{34}$$

and completes the proof of the second part of Theorem 3.

Remark 31. *As with Theorem 1, (34) is stronger than the asymptotic formula stated in part (ii) of Theorem 3, as it provides us with explicit error terms. Moreover, when q odd, $r=2$, $\gamma=2$, and $K=k$, the methods of* [CoSh] *lead to the improved formula*

$$\frac{1}{q^x}\sum_{\substack{\wp\in\mathcal{P}_\psi\\ \deg\wp=x}}|d_{2,\wp}(\psi)|_\infty=\frac{q^x}{x}\sum_{d\in A^{(1)}}\frac{c_d(x)}{[k(\psi[d]):k]}\sum_{\substack{m,n\in A^{(1)}\\ mn=d}}\frac{\mu_A(m)}{|n|_\infty}+\mathrm{O}_{\psi,k}\left(q^{\frac{3x}{4}}\right).$$

7. Concluding remarks

Remark 32. Our main results have been motivated by the study of the elementary divisors of the reductions of an elliptic curve E over $\mathbb{Q}$. One could summarize the emerging tool used for proving (2) and (4) as a Chebotarev Density Theorem for infinitely many number fields, namely as

$$\sum_{m\in\mathbb{N}}\#\{p\le x:\ p\text{ splits completely in }\mathbb{Q}(E[m])/\mathbb{Q}\}\sim\pi(x)\sum_{m\in\mathbb{N}}\frac{1}{[\mathbb{Q}(E[m]):\mathbb{Q}]},\tag{35}$$

unconditionally if $\mathrm{End}_{\overline{\mathbb{Q}}}(E)\not\simeq\mathbb{Z}$ ([Mu]) and provided a $\frac{3}{4}$-quasi GRH holds otherwise ([Co1]). One could ask what the error terms in the asymptotic (35) are, a question that has already been investigated in relation to the study of the distribution of $d_{1,p}(E)$ (see [Co3] for a survey of results). The best error terms are obtained under the full strength of GRH and are $\mathrm{O}_E\left(x^{\frac{3}{4}}(\log x)^{\frac{1}{2}}\right)$ if $\mathrm{End}_{\overline{\mathbb{Q}}}(E)\not\simeq\mathbb{Z}$, and $\mathrm{O}_E\left(x^{\frac{5}{6}}(\log x)^{\frac{2}{3}}\right)$ if $\mathrm{End}_{\overline{\mathbb{Q}}}(E)\simeq\mathbb{Z}$ (see [CoMu]). Our present Theorem 2 may be viewed as the Drinfeld module analogue of (35).

Remark 33. Before investigating the Drinfeld module analogues of (2), (4) and (35), it is natural to consider their analogues in the context of an elliptic curve E over a global function field $\mathscr{K}$. This is precisely the content of [CoTo], where the authors make use of the properties of the division fields of $E/\mathscr{K}$, due to J-I. Igusa, to derive the exact analogues of (2), (4) and (35). For clarity, they essentially prove that, given

a function field $\mathscr{K}$, with field of constants $\mathbb{F}_q$, and given an elliptic curve E over $\mathscr{K}$, with $j(E) \notin \mathbb{F}_q$, then, for any $x \in \mathbb{N}$ such that $x \to \infty$,

$$\sum_{m\in\mathbb{N}} \#\{\wp \in \mathrm{Spec}(\mathscr{K}) : \deg_{\mathscr{K}}(\wp) = x, \wp \text{ splits completely in } \mathscr{K}(E[m])/\mathscr{K}\} = \frac{q^x}{x} \sum_{\substack{m\in\mathbb{N}\\ m|q^x-1}} \frac{c_m}{[\mathscr{K}(E[m]) : \mathscr{K}]} + \mathrm{O}_{E,\mathscr{K},\varepsilon}\left(\frac{q^{x\left(\frac{1}{2}+\varepsilon\right)}}{x}\right), \quad (36)$$

for any $\varepsilon > 0$, where $\mathscr{K}(E[m])$ denotes the m-division field of E and c_m is defined by $\mathscr{K}(E[m]) \cap \overline{\mathbb{F}}_q = \mathbb{F}_{q^{c_m}}$. The asymptotic formula (36) is unconditional and is a direct consequence of the effective Chebotarev Density Theorem for function fields, no extra sieving being required. This special simplification occurs thanks to the inclusion $\mathscr{K}\mathbb{F}_{q^{c_m}} \subseteq \mathscr{K}(E[m])$, and hence to the emerging strong restriction $m|q^x - 1$ in the sum over m needed to be investigated, which does not happen when studying the same problem in the context of elliptic curves over number fields or of generic Drinfeld modules.

Remark 34. In view of the above remarks and parallels between the different settings, it is natural to ask what the best error terms in the asymptotic (22) leading to Theorem 3 might be. For $r \geq 4$, our methods give rise to a dominant error term $\mathrm{O}_{\psi,K,d}\left(q^{\frac{(r+2)c_K x}{2r}}\right)$, which, as $r \to \infty$, is of the same order of magnitude as the one in (36) and as the best error term with respect to x in the standard Chebotarev Density Theorem 28 applied to one (or finitely many) field(s). But what is the true order of magnitude of the error term for *small* r? When $r = 2$, we obtain $\mathrm{O}_{\psi,K,d}\left(q^{\frac{5}{6}c_K x}\right)$, which is the exact analogue of the (conditional upon GRH) error term in (35). However, by making better use of the properties of Drinfeld modules with a non-trivial endomorphism ring, in [CoSh] we succeed in lowering this error term to $\mathrm{O}_{\psi,K,d}\left(q^{\frac{3}{4}x}\right)$ if $\psi \in \mathrm{Drin}_A(k)$ has rank 2 and is such that $\mathrm{End}_{\overline{k}}(\psi)$ is a maximal A-order in a field extension of k of degree 2. We plan to investigate other cases in future work.

Remark 35. It is natural to investigate the positivity of the constants $\delta_{\psi,K}(d)$ and $c(\psi, K)$ appearing in Theorems 1 and 3. The methods involved for such a study are of a completely different nature than the ones used in the present paper and as such will be addressed in future work. Nevertheless, one can already exhibit Drinfeld modules for which some of these densities are positive. For example, the Drinfeld module $\psi \in \mathrm{Drin}_A(k)$ defined by

$$\psi_T = T + \tau - T^{q-1}\tau^2$$

was carefully studied by D. Zywina [Zy], who showed that ρ_ψ has image as large as possible. Consequently, one deduces that

$$\delta_{\psi,k}(d) = \prod_{\substack{\ell\in A^{(1)}\\ \ell \text{ prime}}} \left(1 - \frac{1}{\#\,\mathrm{GL}_2(A/\ell dA)}\right) > 0.$$

Finally, a positivity criterion for the density in Theorem 2 for $d \in \mathbb{F}_q^*$ and ψ having a trivial endomorphism ring was also investigated by W. Kuo and Y-R. Liu in [KuLi, Theorem 3, p. 4]. While we suspect that their

criterion is true, the argument given by the authors contains an error which seems difficult to fix. Indeed, the conclusion of [KuLi, Lemma 14, p. 13] is correct provided that the hypothesis is stronger than that stated: in their notation, one should have $K'_{m'_1} \cap K'_{m'_2} = K$ for any (not necessarily prime, but coprime) m'_1, m'_2 composed of primes of $\mathcal{L}'$. This hypothesis makes the argument of [KuLi, Lemma 15, p. 14], hence also the one of [KuLi, Theorem 3', p. 13], incomplete.

Acknowledgments. Some of the work on this paper was done while A.C. Cojocaru was a member at the Institute for Advanced Study in Princeton, USA, and a guest researcher at the Max Planck Institute for Mathematics in Bonn and the University of Göttingen, Germany. She is grateful to all institutes for excellent work facilities and funding. In particular, she is grateful for research support from the National Science Foundation under agreements No. DMS-0747724 and No. DMS-0635607, and from the European Research Council under Starting Grant 258713.

Both authors are grateful to G. Böckle, F. Breuer, I. Chen, J. Long-Hoelscher, M. Papikian, and D. Thakur for helpful discussions related to the background on Drinfeld modules.

References

[Br] F. Breuer, *Torsion bounds for elliptic curves and Drinfeld modules*, Journal of Number Theory 130, 2010 no. 5, pp. 1241-50.

[Co1] A.C. Cojocaru, *On the cyclicity of the group of $\mathbb{F}_p$-rational points of non-CM elliptic curves*, Journal of Number Theory 96, 2002, pp. 335-350.

[Co2] A.C. Cojocaru, *Cyclicity of CM elliptic curves modulo p*, Transactions of the American Mathematical Society 355, 2003, pp. 2651-2662.

[Co3] A.C. Cojocaru, *Questions about the reductions modulo primes of an elliptic curve*, Number Theory, CRM Proceedings Lecture Notes 36, Amer. Math. Soc., Providence, RI, 2004. pp. 61–79.

[CoMu] A.C. Cojocaru and M.R. Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem*, Mathematische Annalen 330, 2004, pp. 601-625.

[CoPa] A.C. Cojocaru and M. Papikian, *A global characterization of the Frobenius in division fields of rank 2 generic Drinfeld modules,* in preparation.

[CoSh] A.C. Cojocaru and A.M. Shulman, *An average Chebotarev density theorem for generic rank 2 Drinfeld modules with complex multiplication,* Journal of Number Theory 133, no. 3, 2013, pp. 897–914.

[CoTo] A.C. Cojocaru and Á. Tóth, *The distribution and growth of the elementary divisors of the reductions of an elliptic curve over a function field,* Journal of Number Theory 132, 2012, no. 5, pp. 953–965.

[Dr] V.G. Drinfeld, *Elliptic modules*, Mat. Sbornik Tom 94 (136), 1974, No. 4, pp. 594–627, 656, English translation Math. USSR Sbornik 23, 1974, no. 4, pp. 561–592.

[Dr2] V.G. Drinfeld, *Elliptic modules II*, Mat. Sbornik 102, 1977, pp. 182–194, 325, English translation Math. USSR Sbornik 31, 1977, no. 2, pp. 159–170.

[Du] W. Duke, *Almost all reductions modulo p of an elliptic curve have large exponent*, C.R. Acad. Sci. Paris, Ser. I 337, 2003, pp. 689–692.

[FrKu] T. Freiberg and P. Kurlberg, *On the average exponent of elliptic curves modulo p,* IMRN no. 7, 2013, 29 pages.

[Ga] F. Gardeyn, *Une borne pour l'action de l'inertie sauvage sur la torsion d'un module de Drinfeld*, Archiv der Mathematik 79, 2002, pp. 241–251.

[Ge] E.-U. Gekeler, *On Finite Drinfeld Modules*, Journal of Algebra 141, 1991, pp. 187–203.

[Go] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse 35, Springer, Berlin, 1996.

[Ha] D. Hayes, *Explicit Class Field Theory in Global Function Fields*, Studies in Algebra and Number Theory vol 6, 1979, pp. 173–217.

[He] G.-J. van der Heiden, *Weil Pairing for Drinfeld Modules*, Monatshefte für Mathematik 143, 2004, pp. 115–143.

[HsYu] L.-C. Hsia and J. Yu, *On Characteristic Polynomials of Geometric Frobenius Associated to Drinfeld Modules*, Compositio Mathematica 122, no. 3, 2000, pp. 261–280.

[Ki] S. Kim, *On the average exponent of CM elliptic curves modulo p,* preprint, http://arxiv.org/abs/1207.6652

[KuLi] W. Kuo and Y.-R. Liu, *Cyclicity of finite Drinfeld modules*, Journal of the London Mathematical Society 80, 2009, pp. 567–584.

[La] S. Lang, *Algebra*, Graduate Texts in Mathematics **211**, Spring-Verlag, New York, 2002.

[Mu] M.R. Murty, *On Artin's conjecture,* Journal of Number Theory 16, 1983, pp. 147–168.

[MuSc] V.K. Murty and J. Scherk, *Effective versions of the Chebotarev density theorem for function fields* , C.R. Acad. Sci. Paris, t. 319, Série I, 1994, pp. 523–528.

[Pi] R. Pink, *The Mumford-Tate conjecture for Drinfeld modules,* Publ. Res. Inst. Math. Sci. 33, 1997, no. 3, pp. 393–425.

[PiRu] R. Pink and E. Rütsche, *Adelic openness for Drinfeld modules in generic characteristic*, Journal of Number Theory 129, 2009, pp. 882–907.

[Ro] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics 201, Springer-Verlag, New York, 2002.

[Sc] R. Schoof, *The exponents of the groups of points on the reductions of an elliptic curve*, Arithmetic algebraic geometry (Texel, 1989), pp. 325-335, Prog. Math. 89, Birkhäuser Boston, Boston, MA, 1991.

[Se] J-P. Serre, *Summaries of courses of the 1977-78 academic year* (French), pp. 67–71, Collège de France, Paris, 1978.

[Sh] A.M. Shulman, *Elementary divisors of reductions of generic Drinfeld modules,* PhD thesis, University of Illinois at Chicago, 2011.

[Tag1] Y. Taguchi, *The Tate conjecture for t-motives,* Proc. American Math. Society 123, no. 11, 1995, pp. 3285–3287.

[Tag2] Y. Taguchi, *On Φ-modules,* Journal of Number Theory 60, 1996, pp. 124–411.

[Tak] T. Takahashi, *Good reduction of elliptic modules*, J. Math. Soc. Japan, 34 (3), 1982, pp. 475–487.

[Tam] A. Tamagawa, *The Tate conjecture for A-premotives,* preprint 1994.

[Th] D. Thakur, *Function field arithmetic*, World Scientific Publishing Co. Pte. Ltd., New Jersey, 2004.

[Wu] J. Wu, *The average exponent of elliptic curves modulo p,* preprint; http://arxiv.org/pdf/1206.5929.pdf

[Zy] D. Zywina, *Explicit Drinfeld modules with maximal Galois action on their torsion points,* preprint; http://www.math.ias.edu/ zywina/papers/DrinfeldExample.pdf

(Alina Carmen Cojocaru)

- Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 322 SEO, Chicago, 60607, IL, USA;
- Institute of Mathematics "Simion Stoilow" of the Romanian Academy, 21 Calea Grivitei St, Bucharest, 010702, Sector 1, Romania

E-mail address, Alina-Carmen Cojocaru: `cojocaru@uic.edu`

(Andrew M. Shulman)

- Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 322 SEO, Chicago, 60607, IL, USA;

E-mail address, Andrew M. Shulman: ashulm2@uic.edu